

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**
(San Francisco)

Date: To Be Noticed

3. Attached to this Declaration and marked as **Exhibit “A.”** is a true copy of the Findings and Recommendation to Grant John Doe’s Motion to Quash 512(h) Subpoena in *In Re: Subpoena of Internet Subscribers of Cox Communications, LLC And Coxcom LLC*. Case No. 23-00426 JMS-WRP. (D. Haw., August 31, 2023).

4. Attached to this Declaration and marked as **Exhibit “B.”** is a true copy of *A Quick Fix for Online Trademark Infringement* in The Federal Lawyer, July 2012.

5. Attached to this Declaration and marked as **Exhibit “C.”** is a true copy of *Freedom of Speech and the DMCA: Abuse of the Notification and Takedown Process*, (2019) 41 E.I.P.R. 71.

6. Attached to this Declaration and marked as **Exhibit “D.”** is a true copy of *The Importance of a Comprehensive Trademark Enforcement Program: The Changing Tides of Trademark Infringement*, NYSBA Inside, Spring/Summer 2016.


7. Attached to this Declaration and marked as **Exhibit “E.”** is a true copy of an article titled *DMCA Notice-and-Takedown Processes: List of Good, Bad, and Situational Practices*, posted on the USPTO’s website at https://www.uspto.gov/sites/default/files/documents/DMCA_Good_Bad_and_Situational_Practices_Document-FINAL.pdf.

8. Attached to this Declaration and marked as **Exhibit “F.”** is a true copy of a FAQ page found on VSCO’s website at <https://support.vSCO.co/hc/en-us/articles/360040916071-Private-profiles-on-VSCO>.

9. Attached to this Declaration and marked as **Exhibit “G.”** is a true copy of an email thread between Mr. Khimji’s former Canadian counsel (Mr. Johnathan Kleiman) and Mr. Zachery Alinder between December 30, 2024 and January 8, 2025.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed on June 2, 2025 in the City of Coquitlam, Province of British Columbia, Canada.



Simon Lin

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF HAWAII

IN THE MATTER OF:

SUBPOENA OF INTERNET
SUBSCRIBERS OF COX
COMMUNICATIONS, LLC AND
COXCOM LLC

)
)
)
) MISC. NO. 23-00263 JMS-WRP
)
)
) FINDINGS AND
) RECOMMENDATION TO GRANT
) JOHN DOE’S MOTION TO QUASH
) 512(h) SUBPOENA
)

FINDINGS AND RECOMMENDATION TO GRANT JOHN DOE’S
MOTION TO QUASH 512(h) SUBPOENA

Before the Court is John Doe’s Motion to Quash Subpoena (Motion).

See John Doe (Doe) Mot., ECF No. 4. Petitioners Voltage Holdings, LLC, Millennium Funding, Inc., Screen Media Ventures, LLC, and Capstone Studios Corp. filed their Opposition on May 29, 2023. See Pet’rs’ Opp’n, ECF No. 6. The Court finds this Motion suitable for disposition without a hearing pursuant to Local Rule 7.1(c). After careful consideration of the relevant legal authority, the Court FINDS AND RECOMMENDS that Doe’s Motion be GRANTED and that Petitioners’ 512(h) subpoena be quashed.¹

¹ Because Petitioners obtained the relevant subpoena in this case on “a freestanding basis independent of a complaint or litigation,” the “subpoena is its own civil case, and the motion to quash is dispositive of the sole issue presented in

BACKGROUND

This case concerns Petitioners' use of the subpoena provision of the Digital Millennium Copyright Act (DMCA), 17 U.S.C. Section 512(h), to identify internet users who the Petitioners believe are infringing on their copyrights.

On April 13, 2023, Petitioners filed an Application for 512(h) Subpoena (Application) to serve on Internet Service Provider (ISP), Cox Communications, LLC and CoxCom LLC (collectively, "Cox"), to discover the names of several Cox subscribers who appear to have been trading files of copyrighted movies using the protocol BitTorrent. See Application for 512(h) Subpoena, ECF No. 1-3, Ex. 2 at 2 (where Petitioners identify the relevant infringement occurring via a BitTorrent protocol).

"BitTorrent is not a software program, but rather describes a protocol—a set of rules governing the communication between computers—that allows individual computers on the Internet to transfer files directly to other

the case -- whether the subpoena should be enforced or not. Once that question is answered, the dispute between the parties is fully decided." In re DMCA Subpoena to Reddit, Inc., 441 F. Supp. 3d 875, 880 (N.D. Cal. 2020). In the absence of consent by all the parties, as is the case here, the Court must address this dispositive issue in the form of a findings and recommendation to the District Court. See id. at 881 (citing 28 U.S.C. § 636(b)(1)(B)-(C)). Accordingly, within fourteen days after a party is served with the Findings and Recommendation, pursuant to 28 U.S.C. § 636(b)(1), a party may file written objections in the United States District Court. A party must file any objections within the fourteen-day period to preserve appellate review of the Findings and Recommendation.

computers.” BMG Rts. Mgmt. (US) LLC v. Cox Commc’ns, Inc., 881 F.3d 293, 298 (4th Cir. 2018). This method of file sharing is commonly known as “peer-to-peer” (P2P) file sharing and contrasts with the traditional method of downloading a file from a central server using a Web browser. See id.

P2P systems allow users to disseminate files stored on their computers to other internet users. See In re Charter Commc’ns, Inc., Subpoena Enf’t Matter, 393 F.3d 771, 773 (8th Cir. 2005). By utilizing this technology, an internet user can directly search the MP3 file libraries of other users, with no web site being involved because the transferred files are not stored on the computers of the ISP providing the P2P users with internet access. See id. (citing Recording Indus. Ass’n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1232 (D.C. Cir. 2003)).

While Cox has not opposed Petitioners’ Application, it appears from other cases and the circumstances of this case that Cox’s role in disseminating the allegedly copyrighted material is confined to acting as a mere “conduit” in the transfer of files through its network including the files at issue in this case. “As a conduit ISP, Cox only provides Internet access to its subscribers. Cox does not create or sell software that operates using the BitTorrent protocol, store copyright-infringing material on its own computer servers, or control what its subscribers

store on their personal computers.” Cox Commc’ns, Inc., 881 F.3d at 299. In other words, Cox merely provides the internet that connects two users so that they are able to exchange allegedly infringing material on their personal computers.

Petitioners’ Subsection 512(h) subpoena (referred to herein as “512(h) Subpoena” or “Subpoena”) was issued on April 13, 2023, demanding certain subscriber information including the names of Cox subscribers associated with several IP addresses, their last known address, last known telephone number, and any electronic mail addresses associated with the subscribers. See Application for 512(h) Subpoena, ECF No. 1-4 at 1.

On May 24, 2023, one of those subscribers, Doe, appearing *pro se*, filed a letter with this Court, which was construed as the present Motion to Quash the 512(h) Subpoena. See Doe’s Mot., ECF No. 4. In the Motion, Doe objects to the Subpoena, stating that he and his family “erroneously forgot to add a password” to their Wi-Fi network and that they do not have the infringing material on their computers. See id. In their Opposition, Petitioners respond to Doe’s objection; however, neither party analyzes whether the 512(h) Subpoena was valid.

DISCUSSION

When analyzing motions to quash 512(h) subpoenas, courts first address the validity of the subpoena. E.g., In re DMCA Subpoena to eBay, Inc., 2015 WL 3555270, at *2 (S.D. Cal. June 5, 2015); Well Go USA, Inc. v. Unknown Participants in Filesharing Swarm Identified by Hash B7FEC872874D0CC9B1372ECE5ED07AD7420A3BBB, 2012 WL 4387420, at *1 (S.D. Tex. Sept. 25, 2012).

I. Validity of 512(h) Subpoena

The DMCA provision governing issuance of a subpoena to identify an infringer, 17 U.S.C. Section 512(h)(1)-(2), provides in part as follows:

(1) Request.--A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.

(2) Contents of request.--The request may be made by filing with the clerk--

(A) a copy of a notification described in subsection (c)(3)(A);

(B) a proposed subpoena; and

(C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.

17 U.S.C. § 512(h)(1)-(2) (emphasis added).

The notice provision in Subsection 512(c)(3)(A) (referred to herein as a “512(c)(3)(A) notice”) requires the following elements in the notification:

- (i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
- (ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.
- (iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is **to be removed or access to which is to be disabled**, and information reasonably sufficient to permit the service provider to locate the material.
- (iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.
- (v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
- (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

17 U.S.C. § 512(c)(3)(A)(i)-(vi) (emphasis added). To comply with the 512(c)(3)(A) notice provision, a notice must contain *all* of the above requirements.

See Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1112 (9th Cir. 2007). This

notification is a mandatory part of the subpoena request and a condition precedent to the issuance of a subpoena because the statute further provides, as the “[b]asis for granting subpoena,” that the notification filed must satisfy the provisions of subsection 512(c)(3)(A). See In re Charter, 393 F.3d at 775 (citing 17 U.S.C. § 512(h)(4)). Therefore, a 512(h) subpoena may only issue upon proof of a notice to an ISP that complies with each provision in Subsection (c)(3)(A) of the DMCA.

While it does not appear that the Ninth Circuit or the District of Hawaii has addressed whether a copyright owner can meet the requirements of Subsection 512(c)(3)(A) (and thereafter obtain a 512(h) subpoena) when dealing with an ISP that merely acts a conduit between two P2P infringers, the District of Columbia and Eighth Circuits have held that it cannot.

In Verizon and In re Charter, the DC Circuit and Eighth Circuit held that a 512(h) subpoena may be issued only to an ISP engaged in *storing* on its servers material that is infringing or the subject of infringing activity. See Verizon, 351 F.3d at 1233 (“We conclude from both the terms of § 512(h) and the overall structure of § 512 that, . . . a [512(h)] subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity.”); In re Charter, 393 F.3d at 777 (“We agree with and adopt the reasoning of the United States Court of Appeals for the District of Columbia

Circuit in Verizon as it pertains to this statutory issue. Thus, because the parties do not dispute that [the ISP's] function was limited to acting as a conduit for the allegedly copyright protected material, we agree § 512(h) does not authorize the subpoenas issued here.”). Twitter and eBay, for example, store information when users post to their platforms and, therefore, may be subject to a 512(h) subpoena to identify a user who is posting infringing material to their platforms. See In re DMCA § 512(h) Subpoena to Twitter, Inc., 2021 WL 6135300, at *2 (N.D. Cal. Dec. 29, 2021); Rosen v. eBay, Inc., 2015 WL 1600081, at *5 (C.D. Cal. Jan. 16, 2015) (discussing how in creating listings, eBay creates a copy of the copyrighted image and stores it on its servers).

In contrast, 512(h) subpoenas have been held to be invalid when issued to ISPs acting as mere conduits. That is, when the infringement complained of is done through P2P file sharing such as through a BitTorrent protocol, the ISP can neither “remove” nor “disable access to” the infringing material because that material is not stored on the ISP's servers. See Verizon, 351 F.3d at 1237 (“We think it clear . . . that § 512(h) applies to an ISP storing infringing material on its servers in any capacity . . . and does not apply to an ISP routing infringing material to or from a personal computer owned and used by a subscriber.”); 17 U.S.C. § 512(c)(3)(A)(iii). No matter what information the copyright owner may provide in

its 512(c)(3)(A) notice, a conduit ISP cannot remove or disable one user's access to infringing material resident on another user's computer because the ISP does not control the content on its subscribers' computer.² See Verizon, 351 F.3d at 1235; see also id. at 1236 (emphasis added) ("The [copyright owner's] notification identifies absolutely no material [the ISP] could remove or access to which it could disable, **which indicates to us that § 512(c)(3)(A) concerns means of infringement *other than* P2P file sharing.**"). In other words, the ISP is powerless to act upon the infringing material.

In sum, the validity of a 512(h) subpoena depends on whether the copyright owner has provided the ISP with a 512(c)(3)(A) notice that meets all of the criteria set forth in each of the subparts 512(c)(3)(A), and any notice to an ISP concerning its activity as a mere conduit cannot satisfy subpart 512(c)(2)(A)(iii) because there is no infringing material to be removed or access to which can be

² The Court notes that others have argued that an ISP can indeed "disable access" to infringing material by terminating the offending subscriber's internet account. See Verizon, 351 F.3d at 1235. However, the D.C. Circuit dispensed with this argument by noting that, in the text of the DMCA, Congress distinguished the concepts of disabling access to infringing material and disabling access to a subscribers' account. See id. "[W]here different terms are used in a single piece of legislation, the court must presume that Congress intended the terms have different meanings." Id. (citation omitted). That Congress distinguished these concepts in the DMCA establishes that terminating a subscriber's account is not the same as removing or disabling access by others to the infringing material resident on the subscriber's computer. See id.

disabled. See Verizon, 351 F.3d at 1236 (“A § 512(h) subpoena simply cannot meet the notice requirement of § 512(c)(3)(A)(iii).”).

In further support of the conclusion that 512(h) subpoenas are not available to serve on ISPs acting as conduits for P2P file sharing infringement, the courts in Verizon and In re Charter focused on the structure of the DMCA. The DMCA creates safe harbors that shield ISPs from liability for copyright infringement. “Each safe harbor applies to a particular ISP function.” In re Charter, 393 F.3d at 775; see also Verizon, 351 F.3d 1229, 1234 (discussing the differences between the four safe harbors). “The first safe harbor, under § 512(a), limits the liability of ISPs when they do nothing more than transmit, route, or provide connections for copyrighted material—that is, when the ISP is a *mere conduit* for the transmission.” In re Charter, 393 F.3d at 775 (emphasis added). “The second safe harbor, under § 512(b), protects ISPs for ‘system caching,’ that is, instances when they provide intermediate and temporary storage of material on a system or network under certain conditions.” Id. “The third safe harbor, under § 512(c), limits the liability of an ISP for infringing material ‘residing on [the ISP’s] system or network at the direction of its users.’” Id. “The fourth safe harbor, under § 512(d), protects an ISP when it merely links users to online locations containing infringing material.” Id.

The notification provision is found within Subsection 512(c), or the storage-at-the-direction-of-users safe harbor. See In re Charter, 393 F.3d at 776. The notification provision is also referenced, however, in two other safe harbors—subsections (b) and (d) - the “system caching” and “linking” safe harbors. See id. Each of these three subsections “protect an ISP from liability if the ISP responds expeditiously to remove, or disable access to, the material that is claimed to be infringing *upon notification* of claimed infringement as described in [§ 512](c)(3).” Id. (emphasis added).

However, the Verizon and In re Charter courts distinguished the safe harbor under Subsection 512(a) - which does not require notification to an ISP that acts as a mere conduit for the transmission—from the safe harbors established under Subsections 512(b)-(d), which do require notification to the ISP. See Maximized Living, Inc. v. Google, Inc., 2011 WL 6749017, at *5 (N.D. Cal. Dec. 22, 2011) (citing In re Charter, 393 F.3d at 776); see also Verizon, 351 F.3d at 1234 (“Notably present in §§ 512(b)-(d), and notably absent from § 512(a), is the so-called notice and take-down provision.”). The Eighth Circuit determined that “**a specific purpose of the notification provision is to allow an ISP, *after notification*, the opportunity to remove or disable access to infringing material and thereby protect itself from liability for copyright infringement.**”

Maximized, 2011 WL 6749017, at *5 (emphasis added) (citing In re Charter, 393 F.3d at 776). “The absence of the remove-or-disable-access provision (and the concomitant notification provision) [in the safe harbor provision of § 512(a)] makes sense where an ISP merely acts as a conduit for infringing material—rather than directly storing, caching, or linking to infringing material—because the ISP has no ability to remove the infringing material from its system or disable access to the infringing material.” In re Charter, 393 F.3d at 776. Based on this analysis of the structure of the statute, a copyright owner may not request a 512(h) subpoena for an ISP which merely acts as a conduit for P2P file sharing. See Maximized, 2011 WL 6749017, at *5 (citing In re Charter, 393 F.3d at 776-77); Verizon, 351 F.3d at 1236 (“[W]e agree with Verizon that § 512(h) does not by its terms authorize the subpoenas issued here.”).

Accordingly, under Verizon and In re Charter, a 512(h) subpoena may not be issued to a conduit ISP for P2P file sharing infringement because a conduit ISP cannot comply with a 512(c)(3)(A) notice as there is no infringing material to be removed or to disable access to, and, further, the 512(c)(3)(A) notice provision was not intended to apply to ISPs acting as mere conduits.

District Courts in the Ninth and Fifth Circuits have agreed with the D.C. and Eighth Circuits’ reasoning for denying issuance of a 512(h) subpoena

when the circumstances involve an ISP acting as a conduit in P2P infringement. See Well Go USA, Inc. v. Unknown Participants in Filesharing Swarm Identified by Hash B7FEC872874D0CC9B1372ECE5ED07AD7420A3BBB, 2012 WL 4387420, at *2 (S.D. Tex. Sept. 25, 2012) (relying in Verizon and In re Charter and stating that “a copyright owner cannot request a subpoena for an ISP which merely acts as a conduit for data.”); id. at *3 (“While this Court acknowledges it is not bound to follow the precedent of Verizon, it finds compelling the statutory analysis employed in Verizon.”); eBay, Inc., 2015 WL 3555270, at *3 (“This Court agrees that allegedly infringing material must be available to be removed for the § 512(c)(3) notification to have any effect. See § 512(c)(3)(A)(iii). This Court also agrees that a DMCA subpoena, without a satisfactory notification being served simultaneously with or subsequent to the notification, is not enforceable.”); Maximized Living, Inc. v. Google, Inc., 2011 WL 6749017, at *6 (N.D. Cal. Dec. 22, 2011) (“This Court agrees with the reasoning of [Verizon] and holds that the subpoena power of § 512(h) is limited to currently infringing activity and does not reach former infringing activity that has ceased and thus can no longer be removed or disabled.”).

Here, this Court also agrees with the reasoning in Verizon and In re Charter. The Court FINDS AND RECOMMENDS that the 512(h) Subpoena be

quashed because, as stated above, subpart 512(c)(3)(A)(iii) required Petitioners to identify in their 512(c)(3)(A) notice to Cox the infringing material that could be removed or access to which can be disabled, which Petitioners could not do because Cox's role in the alleged infringement was limited to providing the internet service that connected P2P subscribers utilizing a BitTorrent protocol to allegedly download and share movies between their personal computers; there was nothing stored on Cox's servers to be taken down. Because Petitioners' 512(c)(3)(A) notice did not comply with subpart 512(c)(2)(A)(iii) (and it needed to comply with each provision of 512(c)(3)(A), see Perfect 10, 488 F.3d at 1112 and In re Charter, 393 F.3d at 775), Petitioners were not entitled to the 512(h) Subpoena.³

While the validity of the 512(h) Subpoena under Verizon and In re Charter was not discussed in their Opposition, Petitioners were aware that the Court may quash the 512(h) Subpoena as invalid because they cited to Verizon and In re Charter in their original Application for the Subpoena—two cases that quashed 512(h) subpoenas to conduit ISPs where the infringement concerned P2P file

³ The Court notes that there are alternative avenues to seeking Doe's identity including a "John Doe" lawsuit, many of which are pending in district courts across the country. In such a lawsuit, Petitioners could file the John Doe suit together with a motion for third-party discovery to identify an otherwise anonymous John Doe defendant.

sharing. See Application for 512(h) Subpoena, ECF No. 1 at 4. Petitioners chose not to analyze why this case is distinguishable from other P2P file sharing infringements cases involving 512(h) subpoenas in their Opposition. At the very least, in citing to Verizon and In Re Charter in their Application, it appears that Petitioners agree that Cox is a conduit ISP.

Based on the foregoing and the reasoning discussed throughout this Findings and Recommendation, the Court RECOMMENDS that the 512(h) Subpoena be quashed.⁴

II. Information Already Received By Petitioners

The Court points out that until the filing of this Findings and Recommendation, there have been no obstacles to prevent Petitioners from making use of any information they already received from Cox as to the other John Doe identities requested in their 512(h) Subpoena. Accordingly, if the District Court adopts this Findings and Recommendation and quashes the 512(h) Subpoena, the Court further RECOMMENDS that Petitioners be ordered to return and/or destroy any information obtained from the Subpoena, to maintain no further record of the

⁴ Because the Court finds and recommends that the Subpoena was not validly issued, the Court does not address Doe's argument that he and his family failed to add a password to their Wi-Fi and that, because of this, the infringers are not Doe and his family but some unknown third-party who accessed their Wi-Fi.

information from the Subpoena, and to make no further use of the subscriber data obtained from the Subpoena. See In re Charter, 393 F.3d at 778.

CONCLUSION

The Court FINDS AND RECOMMENDS that the 512(h) Subpoena, ECF No. 3, be QUASHED and that Petitioners be ordered return and/or destroy any information derived from the Subpoena, to maintain no further record of the information obtained the Subpoena, and to make no further use of the subscriber data obtained from the Subpoena.

Additionally, the Court ORDERS Petitioners to serve a copy of this Findings and Recommendation on Cox Communications, LLC and CoxCom LLC with instructions for each to provide this Findings and Recommendation to John Doe, I.P. Address: 50.159.108.38.

IT IS SO FOUND AND RECOMMENDED.

DATED AT HONOLULU, HAWAII, AUGUST 31, 2023.



A handwritten signature in black ink, appearing to read "Wes Reber Porter".

Wes Reber Porter
United States Magistrate Judge

IN THE MATTER OF: SUBPOENA OF INTERNET SUBSCRIBERS OF COX COMMUNICATIONS, LLC AND COXCOM LLC; MISC, NO. 23-00263 JMS-WRP; FINDINGS AND RECOMMENDATION TO GRANT MOTION TO QUASH 512(H) SUBPOENA

EXHIBIT B

IP Insight

DEBORAH A. WILCOX AND COURTNI E. THORPE

A Quick Fix for Online Trademark Infringement

Trademark infringements are pervasive on the Internet. One recent scam involves fake offers for free or discounted goods and services in exchange for posting links and “liking” something on Facebook. These scammers use the trademarks of well-known companies in a variety of industries—from airlines to restaurants—to publicize offers on websites that look legitimate when they are not. The unauthorized uses of the trademarks cause confusion among consumers and constitute trademark infringement, among other things. Companies are taking action to protect their brands from this kind of abuse.



One of the most efficient and cost-effective means of addressing these scams is by contacting the Internet service providers (ISPs) to ask them to remove the content or otherwise disable access to the sites where the infringements occur. Many ISPs have developed acceptable use policies that prohibit trademark infringement and provide for infringing material to be taken down when trademark owners report violations. This article discusses best practices for handling removal of material infringing on trademarks from websites.

The Digital Millennium Copyright Act: A Workable Framework

There is no particular trademark law that specifies how ISPs should react to notices of trademark infringement. Although the Digital Millennium Copyright Act (DMCA) has been in effect since 1998 to address copyright infringement online and the liability of ISPs hosting such content, no parallel legislation exists specifically to address these issues in the trademark area. The DMCA procedure is instructive, though, in establishing best practices for handling material that infringes a trademark.

Under the DMCA, every ISP has a duty to develop a policy and procedures for the removal of infringing material from websites it controls and operates on its servers. To comply with the DMCA, an ISP must take down infringing material upon receiving proper notice from the copyright owner. Generally, upon receiving this notice, the ISP will take down the infringing material and forward the notice to the website owner, who will then have an opportunity to present a counter-notice if it claims the material does not infringe copyright. Then, if the copyright owner does not file a lawsuit to protect his or her rights, the ISP is required

to restore the material to the website.¹

Many ISPs have voluntarily extended their DMCA policies and procedures to cover trademarks in addition to copyrights, and they will generally respond to a takedown notice based on trademark rights by either removing the infringing material or disabling the website. This became commonplace in the wake of the 2008 decision made by the Second Circuit Court of Appeals in *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 94 U.S.P.Q.2d 1188 (2d Cir. 2010). In *Tiffany v. eBay*, the Second Circuit held that ISPs charged with hosting websites that infringe on a third party's trademark rights may face liability for contributory infringement if they continue to provide server space to the infringer despite knowing about the infringement. The district court found that eBay's practice of promptly removing challenged listings after receiving notices of trademark infringement protected it from contributory liability, and the Second Circuit Court of Appeals agreed.

Identification of the Correct Internet Service Provider

The most difficult step in the takedown process often may be locating the correct ISP that is providing the hosting services and server space for the infringing site. The first step is to identify the IP address for the infringing site. The starting point should be the WHOIS record for the domain name in question. Each registrar is required to maintain a WHOIS database, and there are some websites that search WHOIS records across many registrars (www.betterwhois.com is one example). At a minimum, the WHOIS record should provide the name of the registrar of the domain name and the name of the domain server. In some cases, the registrar may also be providing the hosting services for the domain name.

The WHOIS record should also have the name and contact information for the owner of the domain name (the registrant), and the name and contact information for an administrator and technical contact person for the domain name. Because many owners of domain names are now using privacy services available through the various registrars, instead of information for an individual or a company, the WHOIS record will indicate that this information is privacy protected. The privacy services generally have terms of service that permit the name and contact information to be disclosed when infringement is alleged. For purposes of sending a takedown notice, it is not necessary to identify the website owner. It is helpful, however, to have this information to establish a pattern of infringement

perpetrated by one individual (some ISPs will disable the infringer's account in cases of repeat offenders) or to follow up with a cease-and-desist letter directly to the individual.

A Domain Information Groper (DIG) search can be conducted on the domain name in order to obtain an IP address for an infringing website.² Free DIG searches are available for individual use at www.kloth.net. Once the IP address is identified, searching the American Registry for Internet Numbers (ARIN) database at www.arin.net will provide the name and contact information for the ISP that has been assigned that particular range of IP addresses. Usually an address or e-mail address for reporting abuse is available from ARIN; however, the information available on ARIN is not always current and accurate.

Another option is to search the list of DMCA-designated agents on file at the U.S. Copyright office, available at www.copyright.gov/onlinesp/list/a_agents.html. As noted above, the DMCA-designated agent often will also be the person who will handle trademark infringement claims for the ISP, or at least the person who would be in a better position to process the notice than others in the company.

Content of the Trademark Takedown Notice

Once the proper ISP is identified, the next step is to review the ISP's trademark policies, which are frequently part of the ISP's Acceptable Use Policy (AUP), Terms of Service (TOS), or Terms of Use. Usually there will be a heading or subheading for Intellectual Property, Copyright, or Trademark Infringement. Many ISPs have simply added trademark claims under the umbrella of their DMCA policy.

As for the content of the takedown notice, if not otherwise specified in the ISP's policy, trademark owners should provide all the information typically found in a DMCA notice:

- the name, contact information, and electronic signature of the person giving notice;
- the URL of the infringing website;
- information sufficient to identify the infringing material;
- a recitation stating a good faith belief that the use of the infringing material is not authorized by the copyright owner or the law; and
- a certification under penalty of perjury that the information in the notice is accurate and that the person submitting the notice is either the copyright owner or the owner's authorized agent.

The notice should also include the basis for demonstrating trademark rights, including any registration numbers or serial numbers assigned by the U.S. Patent and Trademark Office. It is also helpful to reference the ISP's specific policy that is being violated.

Another best practice is to be sure to word the trademark takedown notice carefully so that it clearly

asserts *trademark* rights and does not run afoul of § 512(f) by citing the DMCA as the authority for the notice. To the extent the infringement entails content that infringes both trademark *and* copyright, it may be prudent to send two separate notices, one dealing just with the trademark issues and one that is strictly a DMCA notice addressing the copyright infringement.

Conclusion

Sending a takedown notice can be a quick and easy way to stop trademark infringement on a particular website. This technique is likely to be most effective against an infringer who is new to Internet marketing and lacks an understanding of the serious nature of trademark rights in the United States. When dealing with professional infringers who make their living by conducting this type of activity, it can be harder to stop them with one takedown notice; it may take several rounds of notices as well as cease-and-desist letters to obtain the desired result. As always, keeping a detailed record of the infringing websites and the steps taken against the infringers will assist if litigation becomes necessary. **TFL**

Deborah A. Wilcox is a partner and office coordinator for Baker Hostetler LLP's Intellectual Property, Technology and Media Practice in Cleveland, Ohio. She manages complex copyright, trademark, and e-commerce litigation and counsels clients on trademark and copyright registration and licensing, anticounterfeiting strategies, and digital media and advertising matters. She is currently serving as the president of the Cleveland Intellectual Property Law Association. Courtnei E. Thorpe is an associate in the Intellectual Property Group at Baker Hostetler LLP in Cleveland, Ohio, where she handles disputes involving online trademark and copyright infringement, counsels clients on IP portfolio management, prosecutes trademark applications, and assists with IP litigation. © 2012 Deborah A. Wilcox and Courtnei E. Thorpe. All rights reserved.

Endnotes

¹It is important to note that the DMCA is limited to copyright protection, and the law prohibits sending false notices requesting the takedown of material that is not protected by copyright or is not infringing copyright. Case law is still developing in this area, but improperly asserting trademark infringement under the DMCA might be considered an abusive copyright claim under § 512(f) of the DMCA. See *Online Policy Group v. Diebold Inc.*, 72 U.S.P.Q.2d 1200 (N.D. Cal. 2004) (sending takedown notices to ISPs when the defendant knew the material in question was not protected by copyright found to be abusive copyright claims under DMCA).

²As explained on www.kloth.net, "The DIG utility (domain information groper) is a Unix tool, which can be used to gather information from the Domain Name System servers."

EXHIBIT C

Freedom of Speech and the DMCA: Abuse of the Notification and Takedown Process

Stephen McLeod Blythe*
University of Strathclyde, Glasgow

© Copyright; Digital technology; Freedom of expression; Internet service providers; Notification; Online infringement; United States

The Digital Millennium Copyright Act's "notice and takedown" process is increasingly referred to as a model solution for content removal mechanisms worldwide. While it has emerged as a process capable of producing relatively consistent results, it also has significant problems—and is left open to different kinds of abuse. It is important to recognise these issues in order to ensure that they are not repeated in future legislation. To that end, this article examines the DMCA with reference to its historical context, and the general issues surrounding the enforcement of copyright infringement claims. It then goes on to discuss the notice and takedown process in detail—along with its advantages, disadvantages, criticisms and praise. Specific examples of the kinds of abuse reported by online service providers are outlined, along with explanations of the statutory construction that allows these situations to continue. To finish, the viability of potential alternatives and proposed changes are discussed.

Introduction

The Internet that we know today is a vastly different place from the Internet of 20 years ago. The famous claim that “legal concepts of property, expression, identity, movement, and context do not apply to us [online]”,¹ made by John Perry Barlow in the Declaration of the Independence of Cyberspace, in retrospect now seems alien, and perhaps even naive.

After two decades of exponential growth, the mysterious “World Wide Web” of yesteryear has now become firmly established as an essential network of global significance, and has thus been substantially co-opted into international legal frameworks. It is the standard medium, not just for everyday social interactions, but also as a powerful commercial business tool, opening up a “vast new area of expression and global communication”.² The immediate nature of online interactions has resulted in the varying technologies of the web credited with playing a major role in contemporary political events,³ including the support of political revolution, and even the ultimate overthrow of governments.⁴

The rapid growth of the online space has brought with it a dizzying “kaleidoscope of changes”,⁵ as well as a myriad of questions about our relationship to, and understanding of, intellectual property. Technological advances have allowed for innumerable digital copies of copyright protected materials to be produced and shared all over the world with little to no distribution costs. As a result, the Internet has become “a major source for the dissemination of intellectual property”.⁶ There are now multiple actors responsible for different levels of enforcement online, rather than any single authority that copyright holders can look to for assistance with infringement claims.⁷ Thus, the challenge of how to deal with the new technological landscape is one that both commercial organisations and legislators alike have had to confront, and it is not something that they have always managed to do particularly well.

This article explores the challenges faced by intellectual property holders, with a specific focus on one of the most significant tools used to combat copyright infringement: the Digital Millennium Copyright Act.⁸ Despite the significant benefits for all parties concerned brought about by the DMCA, it has many critics, and is far from perfect. The statutory procedures are by their nature left open to abuse, and despite lying at the very heart of the Internet’s development, the issue of how to effectively tackle copyright infringement online remains, to this day, one of the most challenging to address.

* LLB (Hons) (University of Glasgow), LL.M, Internet Law & Policy (University of Strathclyde). E-Commerce and Privacy LL.M Course Co-Ordinator (University of Strathclyde). Community Guardian (Automatic).

¹ J. Barlow, “Declaration of the Independence of Cyberspace” (2016), <https://www.eff.org/cyberspace-independence> [Accessed 14 December 2018].

² N. Netanel, *Copyright’s Paradox: Property in Expression/Freedom of Expression* (Oxford: 2008), Google Play ebook edition, pp.5, 87.

³ See the discussion of social media’s role on the 2011 English riots: S.A. Baker, “From the criminal crowd to the ‘mediated crowd’: the impact of social media on the 2011 English riots” (2012) 11 *Safer Communities* 1.

⁴ S. Harlow and T.J. Johnson, “Overthrowing the Protest Paradigm? How the New York Times, Global Voices and Twitter Covered the Egyptian Revolution” (2011) 5 *International Journal of Communication* 1359.

⁵ J. Sundell, “Tempting the Sword of Damocles: Reimagining the Copyright/DMCA Framework in a UGC World” (2011) 12 *Minn. Journal of Law, Science, and Technology* 335.

⁶ Y. Tian, “Problems of Anti-Circumvention Rules in the DMCA & More Heterogeneous Solutions” (2005) 15 *Fordham Intellectual Property, Media and Entertainment Law Journal* 749, 750.

⁷ B. Farrand, “Regulatory Capitalism, Decentered Enforcement, and its Legal Consequences for Digital Expression: The Use of Copyright Law to Restrict Freedom of Speech Online” (2013) 10 *Journal of Information Technology & Politics* 408, para.4.

⁸ Herein DMCA.

Intellectual property, the Internet, and freedom of speech

In the United States, copyright holders have a variety of rights conferred upon them under 17 USC §106 including the exclusive rights to reproduction,⁹ the preparation and distribution of both copies¹⁰ and “derivative works”,¹¹ as well as the public performance¹² and display of those works.¹³

From one perspective, copyright may be seen as the ultimate enemy of free speech, restricting the open transfer of common human knowledge and experience in order to protect the self-interest of the few. Taking this view, the Internet can therefore only reach its “free speech potential” if the enforcement of copyright has no place online.¹⁴ To others, copyright law is the very “engine of free expression”,¹⁵ with its core purpose to “promote the creation and publication of free expression”.¹⁶ In other words, copyright is the mechanism by which content creators can safeguard commercial return on their efforts, thus incentivising the creation of new works in the first place.

Irrespective of the natural division between these two perspectives, it would appear self-evident that a “strong copyright system” also comes at a cost to the rights of others.¹⁷ One cannot restrict the dissemination of material to particular actors without impacting on the freedom of another to make use of that same material. As a consequence, critics have argued that there has been a “denial of the relevance of free speech considerations” in relation to current copyright law.¹⁸ Not all share this perspective of course, with some claiming that copyright is really only concerned with the protection of commercial interests in “trivial entertainment products”,¹⁹ and as such poses no threat to genuine freedom of expression.

Irrespective of the view that one takes on the ideological clash between copyright holders and proponents of greater freedom of speech provisions, the dynamic introduced by the development of the Internet to the different actors involved in the creation, use, and dissemination of copyrighted content “adds a vast new dimension”²⁰ to the inherent tension between copyright and free speech. Now, we see courts being asked to apply

the basic principles of copyright “to circumstances that traditional copyright doctrine did not anticipate”²¹—something that arguably extends far beyond its application to “trivial entertainment products”.

The DMCA

Congress enacted the DMCA in 1998 in order to confront some of the growing challenges being faced by the rapid technological development of the time. During this process, the House Committee on Commerce noted that the main goal of the legislation was to promote the growth of a digital economy, and to do so while respecting the rights of intellectual property holders.²² In other words, the DMCA was designed to “serve several masters”,²³ with the law architected carefully in an attempt to “satisfy both sides”²⁴ of the issue: copyright holders, and operators of online platforms. The primary focus of this paper is the DMCA’s “notification and takedown” mechanism, contained within §512.

Safe harbour

The DMCA provides certain categories of online service providers with a “safe harbour”²⁵ from liability for the infringing actions of their users, provided they comply with some specific requirements. These include adhering to the notification and takedown process, the details of which will be outlined in a following section. The safe harbour protection came about as the result of an understanding of the increasing potential for service providers to face litigation from copyright holders for the activities taking place on their platforms,²⁶ and also out of concern about the potential negative impact this would have on economic development in the emerging technological era. The resulting compromise left the responsibility for tracking down instances of unauthorised use of their intellectual property with the right holders themselves, rather than with the host of the content.²⁷ In other words, the DMCA did not impose an obligation on service providers to proactively hunt down allegedly infringing content.

⁹ 17 USC §106(1).

¹⁰ 17 USC §106(3).

¹¹ 17 USC §106(2).

¹² 17 USC §106(4) and (6).

¹³ 17 USC §106(5).

¹⁴ Netanel, *Copyright's Paradox* (2008), p.2, para.3.

¹⁵ *Harper & Row, Publishers Inc v Nation Enterprises Inc* 471 U.S. 539 (1985).

¹⁶ *Eldred v Ashcroft* 537 U.S. 186 (2003), p.34 para.2.

¹⁷ Michael D. Birnhack, *Tel Aviv University Law Faculty Papers* (2008), Paper 56. p.1280 para.2, <http://law.bepress.com/taulwps/art56/> [Accessed 18 December 2018]

¹⁸ See above, p.1281, para.1.

¹⁹ Netanel, *Copyright's Paradox* (2008), p.27, para.1.

²⁰ Netanel, *Copyright's Paradox* (2008), p.22, para.2.

²¹ Netanel, *Copyright's Paradox* (2008), p.70.

²² Report of the House Committee on Commerce, H.R. Rep. No.105-551, Pt 2, pp.22–23 (1998).

²³ David Nimmer, “A Riff on Fair Use in the Digital Millennium Copyright Act” (2000) 148 *University of Pennsylvania Law Review*, p.703 para.1.

²⁴ A. Hassanabadi, “Viacom v. YouTube – All Eyes Blind: The Limits of the DMCA in a Web 2.0 World”, (2011) 26 *Berkeley Technology Law Journal*, p.411, para.3.

²⁵ While the DMCA refers to a “safe harbor”, for the purposes of this article I will be using the UK English spelling of “harbour” unless quoting.

²⁶ A. Hassanabadi, “Viacom v. YouTube – All Eyes Blind: The Limits of the DMCA in a Web 2.0 World”, (2011) 26 *Berkeley Technology Law Journal*, para.1.

²⁷ A. Hassanabadi, “Viacom v. YouTube – All Eyes Blind: The Limits of the DMCA in a Web 2.0 World”, (2011) 26 *Berkeley Technology Law Journal*, p.412, para.2.

In order to qualify for safe harbour, online service providers must register a “designated agent” to act as the recipient of copyright takedown notifications.²⁸ Their name, address, phone number, and email address must be made available publicly, including on the organisation’s website.²⁹ It must also be registered with the US Copyright Office,³⁰ which had over 66,000 designated agents listed as of February 2015.³¹ As of December 2016, registrations must be submitted electronically, and all prior registrations had to be updated by 31 December 2017.³² This change led to concerns that many site operators would unwittingly lose their safe harbour protections.³³

In addition to removing infringing content upon receipt of a valid takedown notification, an online service provider is also required to adopt a policy to suspend or otherwise terminate the accounts of “repeat infringers”.³⁴ The specifics of the implementation are left up to the service provider, but this does not give them unlimited discretion. This point was illustrated in the case of *Disney v Hotfile*,³⁵ where the lack of an effectively implemented policy was central to the eventual loss of the file sharing service’s safe harbour. In the words of the court,

“while the statute does not require Hotfile to maintain a perfect policy ... it is apparent that Hotfile effectively did nothing to tie notices to repeat infringers.”³⁶

Instead, they relied on their own judgment, only suspending the accounts of 43 users out of over 8 million takedown notifications.³⁷ A combination of this inaction, coupled with “the scale of the [infringing] activity” that was occurring on their platform, meant that they did not meet the requirements to qualify for safe harbour under the DMCA.

Another requirement is that service providers must not have either actual knowledge of infringing material on their platform, or circumstances that they could reasonably infer that infringing activity was taking place, known as “red flag” knowledge.³⁸ The case of *Viacom v*

*YouTube*³⁹ brought about an important test of the safe harbour protections in this regard, with Viacom suing the popular video sharing platform’s operators, contending that they were liable for both direct and contributory copyright infringement.⁴⁰ The initial summary judgement went in YouTube’s favour, with the court recognising their right to safe harbour as an intermediary under the DMCA.⁴¹ After this judgment, the liability of service providers with regard to the red flag test has been reduced to the extent that it has been said there would need to be an “immense, crimson banner” before it would trigger a further obligation on them to investigate.⁴²

Notification and takedown process

The notification and takedown process is central to the operation of the DMCA, and provides one of the key compromises between the competing interests of the interested parties. It aimed to achieve this by establishing a standard process to have infringing material efficiently removed from the Internet, without the need to have a court intervene in the first instance.⁴³

Notification and takedown itself involves a number of different parts, in a procedure that has been compared to a “complicated game of tennis”.⁴⁴ First, the complainant must submit a “takedown notification” to the host of the content that conforms to the formal requirements set out in the DMCA. In order to be considered valid, it must contain six specific elements.

These are:

- A signature of someone authorised to act on behalf of the copyright holder (either physical or electronic).⁴⁵
- An identification of the copyrighted works that are allegedly being infringed.⁴⁶
- An identification of where the infringing material is located.⁴⁷
- Information to allow the service provider to contact the complainant (such as name, address, telephone number, email address).⁴⁸

²⁸ 17 USC §512(c)(2).

²⁹ 17 USC §512(c)(2).

³⁰ 17 USC §512(c)(2).

³¹ See http://www.copyright.gov/onlinesp/list/a_agents.htm [Last accessed 28 February 2014].

³² 37 CFR §201.38.

³³ E. Harmon, “Copyright Office Sets Trap for Unwary Website Owners” (1 November 2016), <https://www.eff.org/deeplinks/2016/11/copyright-office-sets-trap-unwary-website-owners> [Accessed 14 December 2018].

³⁴ 17 USC §512(i)(1)(A).

³⁵ Case No.11-20427-CIV-WILLIAMS, <http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1588&context=historical> [Accessed 14 December 2018].

³⁶ Case No.11-20427-CIV-WILLIAMS, p.44, para.2.

³⁷ Case No.11-20427-CIV-WILLIAMS, p.44, paras 2–4.

³⁸ Sundell, “Tempting the Sword of Damocles” (2011) 12 Minn. Journal of Law, Science, and Technology 335, 345, para.1.

³⁹ No. 07 Civ. 2103.

⁴⁰ Hassanabadi, “Viacom v. YouTube – All Eyes Blind: The Limits of the DMCA in a Web 2.0 World”, (2011) 26 Berkeley Technology Law Journal, p.422, para.1.

⁴¹ Hassanabadi, “Viacom v. YouTube – All Eyes Blind: The Limits of the DMCA in a Web 2.0 World”, (2011) 26 Berkeley Technology Law Journal, p.406, para.3.

⁴² Hassanabadi, “Viacom v. YouTube – All Eyes Blind: The Limits of the DMCA in a Web 2.0 World”, (2011) 26 Berkeley Technology Law Journal, p.417, para.1.

⁴³ J. Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure: Misuses, Abuses, and Shortcomings of the Process” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 388, para.1.

⁴⁴ B. Boyden, “The Failure of the DMCA Notice and Takedown System: A Twentieth Century Solution to a Twenty-First Century Problem”, Center for the Protection of Intellectual Property, George Mason University School of Law (2013).

⁴⁵ 17 USC §512(c)(i).

⁴⁶ 17 USC §512(c)(ii).

⁴⁷ 17 USC §512(c)(iii).

⁴⁸ 17 USC §512(c)(iv).

- A “good faith belief” that the material’s use is not authorised by the copyright owner, agent or the law.⁴⁹
- A statement that the notification is “accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of” the copyright holder.⁵⁰

There are also a number of additional qualifications regarding the requirements, where the wording leaves room for interpretation. For example, §512(c)(i) requires that the signature of the authorised party be from a “person”, whereas the other clauses talk about the complaining “party”. If drafted intentionally, then this distinction suggests that while rights can be owned by an organisation, the notification must be signed by an individual acting on their behalf. Interestingly enough, there is no requirement that the person be named at all anywhere else in the takedown notification, outside of the signature. As the statute itself is unclear on this point, it raises the question of how online service providers are supposed to identify whether an illegible (and therefore non-electronic) signature is indeed of a person, and if a notice may be safely rejected as invalid if there is doubt.

In §512(c)(iv), the DMCA specifies that the complaining party must provide information that is “reasonably sufficient” for the service provider to be able to contact them. This includes a telephone number, address, or email address—but it does not state that all of these are required, or indeed that any more than one piece of information needs to be supplied. As a result, it would seem that a takedown notification that only included an email address would be valid.

Another requirement of the notification and takedown process is that the service provider must “remove or disable access to” the material that is identified by a complainant as infringing. While *prima facie* this obligation may seem clear, the specifics of to what extent material should be removed are unclear. In other words, there is no guidance to be found in the statute on whether it is sufficient for material to simply be removed from public availability, or whether the user that uploaded the material in the first place should be refused access. Far from just a trivial matter of implementation, this question has significant implications depending on interpretation. If allegedly infringing material is left accessible to the original uploader, then they are then conceivably free to download and then re-distribute it on another platform. However, should access be removed completely, then the

user could find themselves locked out even in cases where content has been removed as the result of an abusive takedown notification, with no equitable recourse.

Counter notification process

Upon being notified by a service provider that material they have uploaded has been removed as the result of a takedown notification, a user may challenge the takedown by submitting a “counter notification”. In order to be formally valid, it must contain the following:

- “A physical or electronic signature of the subscriber”.⁵¹
- An “identification of the material that has been removed” as the result of the DMCA takedown notification, and where it was located before access was disabled or removed.⁵²
- “The subscriber’s name, address, and telephone number”.⁵³
- “A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled”.⁵⁴
- “A statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber’s address is outside of the United States, for any judicial district in which the service provider may be found”.⁵⁵
- A statement that “the subscriber will accept service of process from the person [who submitted the takedown notification]” or their agent.⁵⁶

Upon receipt of a valid counter notification, the service provider is to then forward it on to the complainant.⁵⁷ If they do not receive notice that legal proceedings have then begun regarding the complaint, then they are to restore access to the material between 10 and 14 business.⁵⁸ Providers are not obliged to honour this process, or to restore access to material upon receipt of a valid response. Rather, doing so means that they cannot be held liable “for any claim based on the service provider’s good faith ... removal of material”.⁵⁹ In practical terms, platforms usually reserve the right to

⁴⁹ 17 USC §512(c)(v).

⁵⁰ 17 USC §512(c)(vi).

⁵¹ 17 USC §512(g)(3)(A).

⁵² 17 USC §512(g)(3)(B).

⁵³ 17 USC §512(g)(3)(C).

⁵⁴ 17 USC §512(g)(3)(D).

⁵⁵ 17 USC §512(g)(3)(D).

⁵⁶ 17 USC §512(g)(3)(D).

⁵⁷ 17 USC §512(g)(2)(B).

⁵⁸ 17 USC §512(g)(2)(C).

⁵⁹ 17 USC §512(g)(1).

terminate accounts or content at any time as part of their Terms of Service,⁶⁰ rendering the likelihood of any successful action questionable.

Fair use and the DMCA

Not all unauthorised use of copyrighted material is considered infringing under US law, with the “fair use doctrine” allowing for exceptions.⁶¹ This acts as “an affirmative defence to a copyright infringement accusation”.⁶² In other words, it “affords a privilege to make what would otherwise be an infringing use of copyrighted expression”.⁶³ The Supreme Court has described fair use as part of the “built-in” protections for freedom of speech that exists in copyright law,⁶⁴ and in *Campbell v Acuff-Rose Music*,⁶⁵ fair use opportunities were said to be “necessary to fulfil copyright’s very purpose”.⁶⁶ Put another way, fair use is seen as a “free speech safety valve”,⁶⁷ helping to reduce the tension between copyright and freedom of speech, and as a result, it is “part of the constitutional fabric of copyright law”.⁶⁸

The fair use doctrine holds that the use of materials for specific purposes, such as “criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research”, will not constitute an infringement of copyright, depending on the manner and context in which they were used.⁶⁹ There are four factors under US law that are to be taken into account when determining whether or not content falls under the fair use protections of 17 USC §107. These are “the purpose and character of the use”⁷⁰; “the nature of the copyrighted work”⁷¹; “the amount and substantiality of the portion used in relation to the copyrighted work as a whole”⁷²; and “the effect of the use upon the potential market for or value of the copyrighted work”.⁷³ Any fair

use adjudication will be based on a balance of the four above factors,⁷⁴ and therefore operate on a “case-by-case basis”.⁷⁵

There are many examples where the use of material online that might otherwise have constituted infringing activity was judged to fall under fair use protections. These include a newspaper that used quotations of controversial “religious” texts for critical purposes⁷⁶; members of an online forum who shared a short excerpt from a newspaper for discussion⁷⁷; and the display of cached versions of websites in search results.⁷⁸

The technology giant Google has built its success on a model that is “heavily reliant on the fair use doctrine”.⁷⁹ In the case of *Perfect 10 v Google*,⁸⁰ the Federal District Court rejected their argument that the use of thumbnails taken from websites in Google’s Image search was fair use.⁸¹ If left to stand, this decision would clearly have had serious implications for the technology sector. However, it was reversed in the later case of *Perfect 10 v Amazon*,⁸² where the Ninth Circuit found that the system involved was “highly transformative”,⁸³ and therefore fell under fair use protections. This decision was said to be “critical to the future of search engines”.⁸⁴

One of the most significant judgments for the relationship between the DMCA and fair use came in *Lenz v Universal Music*,⁸⁵ also known as the “dancing baby” case. Having shared a home recording of her young son dancing to a Prince song on YouTube, the complainant, Stephanie Lenz, then found it had been removed soon after as the result of a takedown notification sent by the artist’s record label.⁸⁶ Lenz took legal action in response, and the court held that as fair use of material constitutes a “lawful use”,⁸⁷ copyright holders have a duty to take this into account before submitting a takedown notification.⁸⁸

⁶⁰ See, for example, s.20 of Tumblr’s Terms of Service at <https://www.tumblr.com/policy/en/terms-of-service> [Accessed 14 December 2018].

⁶¹ Sundell, “Tempting the Sword of Damocles” (2011) 12 Minn. Journal of Law, Science, and Technology 335, 342, para.2.

⁶² A.C. Brannan, “Fair Use Doctrine and the Digital Millennium Copyright Act: Does Fair Use Exist on the Internet Under the DMCA?” (2001) 42 *Santa Clara Law Review* 247, para.3.

⁶³ Netanel, *Copyright’s Paradox* (2008), p.76.

⁶⁴ *Eldred v Ashcroft* 537 U.S. 186 (2003), p.29, para.2.

⁶⁵ *Campbell v Acuff-Rose Music* 510 U.S. 569 (1994).

⁶⁶ *Campbell v Acuff-Rose Music* 510 U.S. 569, 575 (1994) at para.1.

⁶⁷ Netanel, *Copyright’s Paradox* (2008), p.77.

⁶⁸ Band, “Google and Fair Use” (2008) 3 *Journal of Business and Technology Law* 1, 7, para.1.

⁶⁹ 17 USC §107.

⁷⁰ 17 USC §107 s.(1).

⁷¹ 17 USC §107 s.(2).

⁷² 17 USC §107 s.(3).

⁷³ 17 USC §107 s.(4).

⁷⁴ Brannan, “Fair Use Doctrine and the Digital Millennium Copyright Act” (2001) 42 *Santa Clara Law Review* 247, 252, para.7.

⁷⁵ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 389 para.3.

⁷⁶ *Religious Technology Center v Lerma* 908 F. Supp. 1362, 1367 (E.D. Va. 1995).

⁷⁷ *Righthaven LLC v Democratic Underground*, No.2:10-cv-01356-RLH (GWF).

⁷⁸ *Field v Google Inc* 412 F. Supp. 2d 1106 (D. Nev. 2006).

⁷⁹ Band, “Google and Fair Use” (2008) 3 *Journal of Business and Technology Law* 1, para.1.

⁸⁰ *Perfect 10 Inc v Google* 416 F. Supp. 2d 828 (C.D. Cal. 2006).

⁸¹ Band, “Google and Fair Use” (2008) 3 *Journal of Business and Technology Law* 1, 13, para.1.

⁸² *Perfect 10, Inc. v. Amazon.com, Inc.* 487 F.3d 701 (9th Circ. 2007).

⁸³ Band, “Google and Fair Use” (2008) 3 *Journal of Business and Technology Law* 1, 15, para.1.

⁸⁴ Band, “Google and Fair Use” (2008) 3 *Journal of Business and Technology Law* 1, 15, para.3.

⁸⁵ *Lenz v Universal Music* 572 F. Supp. 2d 1150 (N.D. Cal. 2008).

⁸⁶ Sundell, “Tempting the Sword of Damocles” (2011) 12 Minn. Journal of Law, Science, and Technology 335, 353, para.2.

⁸⁷ K. O’Donnell, “Lenz v. Universal Music Corp. and the Potential Effect of Fair Use Analysis Under the Takedown Procedures of §512 of the DMCA” (2009) 10 *Duke Law & Technology Review* 9, para.22, available at <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1194&context=dltr> [Accessed 14 December 2018].

⁸⁸ See above.

Benefits and criticisms of the DMCA

Benefits of the DMCA

Aiming to find a workable legal compromise between a multitude of competing actors is a lofty goal, and it appears that, for all of its flaws, the DMCA has at least got something right. The notification and takedown process is now seen as the “go-to model” for dispute resolution, adopted in various forms in legal systems outside of the US.⁸⁹

A well-structured copyright system is of benefit to society, both for freedom of speech, and the economy. A report in 2007 estimated that there was a loss of \$12.5 billion to the US economy every year from the piracy of sound recordings alone,⁹⁰ a loss of 71,060 jobs,⁹¹ and that the various levels of the American Government were losing a “minimum of \$422 million in tax revenues annually”.⁹²

Copyright is not just important to major industry groups, but is also “an integral part of our system of freedom of expression”.⁹³ The power to control the use of, and exploit, intellectual property supports artists, musicians, painters, writers and others to create new works in a sustainable manner. Copyright helps ensure that content creators are recognised for their contributions, as well as having the option to benefit financially from them. In addition, it also means that they retain the ability to prevent the use of works for purposes that are not compatible with the original intent, such as musicians refusing to allow their tracks to appear as part of political rallies, or in advertising.⁹⁴

The ability to have infringing content removed quickly from the Internet in an age where multiple copies can be created in seconds is a must, and the DMCA provides a straightforward mechanism for this to take place, with online service providers tasked with removing infringing content “expeditiously” upon receipt of a valid takedown notification.^{95 96}

If we look solely at the volume of takedown requests issued by intellectual property holders to online service providers, it would appear that they have embraced the DMCA as a compromise to the problem of copyright infringement. In 2013 alone, Google reportedly received 235 million such notifications, with 9 per cent of them rejected for being invalid, or duplicates.⁹⁷ In just a single month from 2014, they reported 4.6 million takedown requests from member companies of the British Phonographic Industry.⁹⁸ The total figure received is increasing year on year, as much as 524 per cent in 2012.⁹⁹ Other companies also report significant engagement with the DMCA process, with Microsoft stating that they issue takedown notifications for “millions of infringing files per year”.¹⁰⁰ Despite changes in the online landscape, the DMCA retains its relevancy to this day.¹⁰¹

Criticisms of the notification and takedown process

The DMCA remains the subject of great controversy,¹⁰² attracting significant criticism from all sides. Chided as belonging to a different era,¹⁰³ it has been described as a system “that makes no one happy”,¹⁰⁴ as well as being “rife with controversy and confusion”.¹⁰⁵ While an efficient process for the removal of content is required, it has been said that attempting to use the provisions of the DMCA to combat copyright infringement even on a single site is akin to “trying to bail out an oil tanker with a thimble”,¹⁰⁶ owing to the sheer volume of infringing activity online. In the face of such a monumental task, DMCA takedown notifications are seen as “flawed and inefficient”.¹⁰⁷

While there are many issues with the DMCA’s notification and takedown procedure, one of the most significant concerns is the unilateral power it grants to copyright holders, which operates without judicial oversight.¹⁰⁸ The process can result in the removal of material irrespective of whether it is being used in a lawful manner or not,¹⁰⁹ and the burden of proof is placed on the subscriber to provide a justification for the

⁸⁹ J. Urban, J. Karaganis and B. Schofield, “Notice and Takedown in Everyday Practice”, *UC Berkeley Public Law Research Paper No.2755628* (2017), version 2, p.19, para.4.

⁹⁰ S.E. Siwek, “The True Cost of Sound Recording Piracy to the U.S. Economy”, Institute for Policy Innovation, Report 118 (2007), p.i.

⁹¹ Siwek, “The True Cost of Sound Recording Piracy to the U.S. Economy” (2007), p.i.

⁹² Siwek, “The True Cost of Sound Recording Piracy to the U.S. Economy” (2007), p.i.

⁹³ Siwek, “The True Cost of Sound Recording Piracy to the U.S. Economy” (2007), p.51, para.2.

⁹⁴ Siwek, “The True Cost of Sound Recording Piracy to the U.S. Economy” (2007), pp.62–63.

⁹⁵ USC 17 §512(c).

⁹⁶ Netanel, *Copyright’s Paradox* (2008), p.128.

⁹⁷ “Google discarded 21,000,000 takedown requests in 2013” (27 December 2013), *TorrentFreak.com*, <http://torrentfreak.com/google-discarded-21000000-takedown-requests-in-2013-131227> [Accessed 14 December 2018].

⁹⁸ Google Transparency Report, <https://www.google.com/transparencyreport/removals/copyright> [Accessed 14 December 2018].

⁹⁹ D. Seng, “The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices” (2014) 18 *Virginia Journal of Law and Technology* 11.

¹⁰⁰ *Amicus Brief of Microsoft Corporation and Electronic Arts Inc. in the case of Viacom International, Inc v YouTube Inc*, p.3, <http://docs.justia.com/cases/federal/appellate-courts/ca2/10-3270/112> [Accessed 14 December 2018].

¹⁰¹ Urban et al., “Notice and Takedown in Everyday Practice” (2017), p.28, para.2.

¹⁰² Brannan, “Fair Use Doctrine and the Digital Millennium Copyright Act” (2001) 42 *Santa Clara Law Review* 247, para.1.

¹⁰³ Boyden, “The Failure of the DMCA Notice and Takedown System”, Center for the Protection of Intellectual Property, George Mason University School of Law (2013).

¹⁰⁴ Boyden, “The Failure of the DMCA Notice and Takedown System”, George Mason University School of Law (2013).

¹⁰⁵ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 *Minn. Journal of Law, Science, and Technology* 387, 394, para.2.

¹⁰⁶ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 *Minn. Journal of Law, Science, and Technology* 387, 394, para.2.

¹⁰⁷ Hassanabadi, “Viacom v. YouTube – All Eyes Blind: The Limits of the DMCA in a Web 2.0 World”, (2011) 26 *Berkeley Technology Law Journal*, p.437, para.3.

¹⁰⁸ Farrand, “Regulatory Capitalism, Decentered Enforcement, and Its Legal Consequences for Digital Expression” (2013) 10 *Journal of Information Technology & Politics* 408, 413, para.3.

¹⁰⁹ J.M. Miller, “Fair Use Through the Lenz of §512(c) of the DMCA: A Preemptive Defense to a Premature Remedy?” (2010) 95 *Iowa Law Review* 1697, 1708, para.3.

publication, resulting in “censorship before adjudication”.¹¹⁰ In other words, website owners or publishers that are the subject of a DMCA takedown notification are in many ways deemed to be guilty before proven innocent.¹¹¹ Effectively, the state provides a framework “with which private citizens are able to silence” others.¹¹² It is perhaps inevitable that any effort to streamline the removal of allegedly infringing content will result in the erosion of the safeguards put in place to protect fair use, but the question is whether or not the discretion offered to right holders is proportionate or not.

The imbalanced nature of the DMCA also has a negative effect on online service providers, despite their safe harbour protections. In order to shield their users from frivolous or illegitimate copyright claims, platforms have to analyse each notice for both completeness and validity, as well as make a judgment call on any fair use argument. This sort of review requires a significant amount of both resources expertise, and for hosts that receive millions of notices, may prove to be impractical.

If a service provider does decide to take a proactive stance in filtering out takedown notifications, they also have to be prepared to risk losing their safe harbour protections in situations where they may refuse to comply with a notice. This is something that few are prepared to do,¹¹³ even in cases where the probability of any resulting litigation is minimal. There would need to be a persuasive commercial argument made in order to make the decision to take on the potential costs that the legal risk would involve.¹¹⁴ As a result of this inherent reluctance, many fraudulent or illegitimate DMCA takedown notifications will inevitably be processed, and content removed without the detailed scrutiny that may show up potential fair use defences. In addition, it has observed that it would be straightforward to force platform operators to shut down by sending multiple DMCA takedown notifications that would require attention to deal with properly.¹¹⁵

One of the other major criticisms of the DMCA is that it does not really solve the core problem of copyrighted material being shared without permission, offering “little protection”¹¹⁶ for holders of intellectual property rights. As one piece of allegedly infringing material is removed as the result of a valid takedown notification, it can simply be re-uploaded by the infringing party elsewhere, in the same form—potentially even on the same platform. Despite this, the safe harbour provisions mean that no action can be taken against the online service provider, so long as they act within the terms of the statute. This situation leads to an endless cat and mouse scenario between the holders of intellectual property rights, and

those abusing them. As a result, the whole thing has been compared to the arcade game “whac-a-mole”, where copyright holders have to guess where the next offending party is going to appear.¹¹⁷ To this end, small-scale copyright holders are at a particular disadvantage under the DMCA, with the “poor protection” that it offers.¹¹⁸ The burden imposed to monitor the Internet for infringement rests especially heavily on their shoulders, compared to larger organisations with significant resources to devote to the task. For this reason, it can be easy to see the DMCA as a tool that only significantly benefits major parties, both in terms of service providers, and copyright holders.

Criticisms of the counter-notification process

As well as general criticisms of §512, there are specific issues in relation to the counter-notification portion of the process, which is “limited in both structure and practice”.¹¹⁹ In some ways, this should perhaps not come as too much of a surprise, as the procedural recourse for subscribers was only incorporated into the DMCA “at the last minute”.¹²⁰

One of the first hurdles is that, in order to have access to allegedly infringing material restored, subscribers are required to submit a valid counter-notification to the service provider. However, to do so they must become aware that access to the disputed material has been disabled in the first place. There is no statutory requirement placed upon service providers to notify users that this has been done, and so users are forced to rely on the relevant platform’s policy decisions, which inevitably vary in their scope, and don’t necessarily include adequate notification.

Secondly (and as mentioned earlier), there is no obligation on a service provider to actually honour the counter-notification process, and, as a result, they may conclude that leaving content down is a more attractive prospect. This scenario seems more likely when we consider that there are practical questions involved in removing content in such a way that it can be restored efficiently at a later date. Reinstating access is not necessarily technically feasible for smaller platforms with limited resources available for developing such bespoke solutions. This creates another imbalance in the notice and takedown mechanism, with one of the key remedies available to subscribers dependent on the willingness of their host to comply.

¹¹⁰ T.A. Lyons, “Scientology or Censorship: You Decide” (2000) Camden Rutgers School of Law Publications (2000), p.19, para.1.

¹¹¹ Sundell, “Tempting the Sword of Damocles” (2011) 12 Minn. Journal of Law, Science, and Technology 335, 356, para.3.

¹¹² Lyons, “Scientology or Censorship: You Decide”, Camden Rutgers School of Law Publications (2000), p.19, para.1.

¹¹³ GartnerG2, “Copyright and Digital Media in a Post-Napster World”, (2003) The Berkman Center for Internet & Society at Harvard Law School, p.27, para.4, available at https://cyber.harvard.edu/wg_home/uploads/254/2003-05.pdf [Accessed 14 December 2018].

¹¹⁴ Netanel, *Copyright’s Paradox* (2008), p.127.

¹¹⁵ *Design Furnishings Inc v Zen Path*, 2:10-02765, 2010 WL 4321568, at *5 (E.D. Cal. 21 October 2010).

¹¹⁶ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 394, para.2.

¹¹⁷ Hassanabadi, “Viacom v. YouTube – All Eyes Blind: The Limits of the DMCA in a Web 2.0 World”, (2011) 26 Berkeley Technology Law Journal, p.406, para.2.

¹¹⁸ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 397, para.3.

¹¹⁹ Urban et al., “Notice and Takedown in Everyday Practice” (2017), p.44, para.2.

¹²⁰ Urban et al., “Notice and Takedown in Everyday Practice” (2017), p.7, para.3.

Should a provider decide that they will accept, and give effect to valid counter-notifications, there are then procedural issues to be considered. Despite the obvious differences in the substantive requirements between the notification and counter notification processes, there are a few additional discrepancies in their *application*. First, as explained earlier, a complainant is only required to provide enough information that is “reasonably sufficient” for a service provider to contact them. In contrast, a subscriber must submit their full name, address and telephone number in order for their counter-notification to be considered valid. This leaves a situation where material can be removed with nothing more than an email address given, with far more information required to have access to that same material restored. Secondly, while takedown notifications can be submitted through a third party acting on behalf of the copyright holder, this option appears unavailable in the case of counter-notifications, as a result of the statute’s requirement that the subscriber’s name, address, telephone number and signature be detailed. Thirdly, there is a clear disparity in the requirement for allegedly infringing content to be removed “expeditiously”, and the minimum of 10 business days before it can be restored upon receipt of a valid counter-notification.¹²¹

These differences result in an imbalance in the DMCA, which leave the system open to abuse. While complainants can have material removed without providing anything more than an email address, or do so through an agent, the subscriber is forced to provide far more information in order to have access to the material reinstated. In the case of fraudulent takedowns, users are then faced with the choice of either giving up their full contact details to a potentially malicious complainant, or else to have their content permanently taken offline. This dichotomy was highlighted by a WordPress.com subscriber, who shared their dissatisfaction with the counter-notification requirements on their blog, after having access to material that they had published disabled. In their view, the initial takedown notification was a fraudulent abuse of the system, but in order to challenge it they were forced to provide personal details to an allegedly dishonest individual:

“WordPress offers customers like me a stark and unrealistic choice: fill in a DMCA ... counter-notice containing precious personal data of great value to the crooks who hack our bank accounts – or be taken down.”¹²²

Another example in the same vein concerns the case of an independent author who found themselves the subject of fraudulent takedown notifications regarding their recently published book. They were also concerned about the requirement to provide their full name address in a counter-notification, stating: “I very much resent the idea that I might be forced to give identifying information to someone who has behaved fraudulently.”¹²³

The anger displayed to the service providers at the prospect of having to provide personal information to the original complainant who filed the takedown notification may well be justified, but is ultimately misplaced. It is the requirements of the DMCA, and not the service provider, that requires a valid counter-notification to be submitted before access to disputed material can be restored. Either way, it demonstrates another aspect of the imbalance in the DMCA’s notification and takedown process, along with the potential for abuse.

The concerns outlined above have been shown to be well founded, and not just theoretical in nature, with a German newspaper reporting that terrorist groups submitted fraudulent takedown notifications to YouTube over content appearing on the channel of an Arabic Christian TV organisation. After counter-notifications were lodged, access to the material was restored, but the operators began to receive death threats, directly as a result of their contact information being passed on as part of the process.¹²⁴

The imbalance of the information required is not the only issue with the counter notification process that leaves it open to abuse. After allegedly infringing material is taken offline by a service provider under the DMCA, access is not immediately restored upon the receipt of a counter-notification, but instead the request is put on hold for a period of “not less than 10, nor more than 14 business days”.¹²⁵ While ultimately content will be restored, this means that the takedown process has the potential to censor legitimate material for at least ten days, and far longer if the site owner does not notice and react immediately. This can cause significant issues,¹²⁶ particularly for time-sensitive pieces (such as those commenting on contemporary events), where the information would be rendered inaccessible for the most critical period in which it would gain exposure. The subsequent loss of both reputation and income for a publisher¹²⁷ makes it easy to see how those with nefarious intent can use the DMCA’s notification and takedown process as an effective censorship tool.

These examples highlight issues that have occurred when the statutory process was followed, but that is not always the case. For example, there are many instances

¹²¹ Urban et al., “Notice and Takedown in Everyday Practice” (2017), p.45, para.3.

¹²² A. Jennings, “Has WordPress Surrendered to the Cybercrooks?” (25 October 2014), <https://transparencyinsportblog.wordpress.com/2014/10/25/has-wordpress-surrendered-to-the-cybercrooks/> [Last accessed 25 October 2014].

¹²³ B. Mills, “Independent Publishing and DMCA Abuse, or ‘How A Scammer Got My Book Blocked With Very Little Effort’” (1 March 2015), *The Active Voice*, <http://the-active-voice.com/2015/03/01/nolander-blocked-at-amazon-and-smashwords/> [Accessed 14 December 2018].

¹²⁴ S. Karish, “Wer hat sie verraten? Googles YouTube-Daten!” (5 November 2014), *Frankfurter Allgemeine*, <http://www.faz.net/aktuell/feuilleton/debatten/YouTubes-daten-gefahrden-islamkritiker-13247806-p3.html?printPageArticle=true> [Accessed 14 December 2018].

¹²⁵ DMCA §512(g)(2)(C).

¹²⁶ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 398, para.2.

¹²⁷ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 398, para.3.

of access to material not being restored within the designated time after the receipt of a valid counter notification. One such occasion involved Chunlou Yung, a fan of a Swedish horror film that was set for an American re-make. Having set up a Facebook group to promote the English release, much of the content was removed as the result of a DMCA takedown notification issued by a group representing the film-makers. Based on a fair use argument,¹²⁸ Yung responded quickly with a counter-notification, but the content remained offline for almost 20 days before Facebook reinstated access—6 days longer than provided for in the DMCA—by which point he had decided to no longer promote the film, and closed down the community.¹²⁹ This demonstrates how publishers are at the mercy of the diligence of online service providers to stick to the timeline laid out in the DMCA, while suffering the consequences of the content being offline, and again highlights the systemic potential for abuse.

Submitting a counter-notification can be a daunting undertaking. Even where users are perfectly entitled to use the material in question, many lack the “tech savvy” required to engage with the process.¹³⁰ Those that do, still have to contend with its legal nature, which can be intimidating. The gravity of the mechanism is something that is emphasised by online service providers, with Twitter describing the action of submitting a counter notification as “serious business”.¹³¹ As a result, subscribers may choose to leave perfectly legitimate content offline, rather than engage in a process that they deem to be too intimidating or legalistic. In practice, counter-notifications are rarely sent,¹³² even where there is a wealth of detailed information available to help subscribers do so.¹³³ For example, Automattic reported that counter-notices were only received in response to 2 per cent of the takedown notifications they received in the period of January to July of 2016.¹³⁴

Such a low level of challenge to DMCA takedown notifications could be seen as an argument that the process is working effectively, removing a significant amount of content without any apparent objection. However, the levels of abusive notices reported by organisations in their transparency reports¹³⁵ would suggest that the situation is not that straightforward. Rather, the number of incomplete

or invalid takedown notifications is significant,¹³⁶ and the imbalances in the notification and takedown procedure allow for it to be used to bully publishers to remove critical content without any real chance of recourse.¹³⁷ The lack of effectiveness in the procedural elements of the counter notification process shown in these criticisms demonstrate the very real potential for there to be a chilling effect on free speech as a result.

Abuse of the DMCA

The previous sections have concentrated largely on issues with the procedural elements of the DMCA, and the effectiveness of them in dealing with copyright infringement. However, in practice, the use of the notification and takedown process is not solely restricted to the expression of legitimate copyright concerns, but also for the purposes of “copyfraud”.¹³⁸ “Examples of abuse abound”,¹³⁹ and “fake assertions of copyright are everywhere”,¹⁴⁰ with the legislation brandished by some complainants as a tool to cut down views that they find to be undesirable. In essence the DMCA is being abused in these circumstances as a means of achieving censorship. Perhaps most damning of all is the assertion that the system itself “encourages these kind of egregious removal requests”,¹⁴¹ and may even lead complainants to perjure themselves in an effort to get content taken offline.¹⁴²

The notification and takedown process has resulted in a substantial amount of material being removed from online distribution, “both infringing and non-infringing”.¹⁴³ This is something demonstrated in transparency reports published by major online service providers, which show that a significant proportion of takedown notifications are subsequently rejected upon receipt for either failing to fulfil the formal requirements, or for being an inappropriate use of the DMCA. Wikipedia reported that only 27 per cent of the takedown notifications they received between January and June 2016 were ultimately processed.¹⁴⁴ WordPress.com removed content in response to 55 per cent of the 4,258

¹²⁸ M. Masnick, “Movie Producers Want Sole Ownership of Facebook Fans” (21 September 2010), *TechDirt*, <https://www.techdirt.com/articles/20100913/20473110993/movie-producers-want-sole-ownership-of-facebook-fans.shtml> [Accessed 14 December 2018].

¹²⁹ J. Bailey, “The Facebook, the DMCA, and the Problem with Counternotices”, (13 October 2010), *PlagiarismToday*, <https://www.plagiarismtoday.com/2010/10/13/the-facebook-the-dmca-and-the-problem-with-counternotices> [Accessed 14 December 2018].

¹³⁰ GartnerG2, “Copyright and Digital Media in a Post-Napster World”, (2003) The Berkman Center for Internet & Society at Harvard Law School, p.28, para.1, available at https://cyber.harvard.edu/wg_home/uploads/254/2003-05.pdf [Accessed 14 December 2018].

¹³¹ See <https://support.twitter.com/articles/15795-copyright-and-dmca-policy#12> [Accessed 14 December 2018].

¹³² Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 391, para.3.

¹³³ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 395, para.3.

¹³⁴ See <https://transparency.automattic.com/intellectual-property/2016-h1> [Accessed 14 December 2018].

¹³⁵ See <https://transparency.automattic.com/intellectual-property/2016-h1> [Accessed 14 December 2018], and see further discussion on this point in the following section.

¹³⁶ A. Neill and E. Lee, “Fixing Section 512 – Legislative Reforms for the DMCA Safe Harbor Provisions” (2016) *American Intellectual Property Law Association Quarterly Journal*, available at <https://ssrn.com/abstract=2879696> [Accessed 14 December 2018].

¹³⁷ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 403 para.2.

¹³⁸ J. Mazzone, “Copyfraud” (2006) 81 *New York University Law Review* 1026.

¹³⁹ Hassanabadi, “Viacom v. YouTube – All Eyes Blind: The Limits of the DMCA in a Web 2.0 World”, (2011) 26 *Berkeley Technology Law Journal*, p.437 para.3.

¹⁴⁰ Mazzone, “Copyfraud” (2006) 81 *New York University Law Review* 1026, 1029, para.1.

¹⁴¹ Sundell, “Tempting the Sword of Damocles (2011) 12 Minn. Journal of Law, Science, and Technology 335, 353, para.2.

¹⁴² Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 400, para.1.

¹⁴³ Netanel, *Copyright’s Paradox* (2008), p.128.

¹⁴⁴ Wikipedia, “Requests for Content Alteration & Takedown”, <https://transparency.wikimedia.org/content.html> [Accessed 14 December 2018].

notifications they received between January and July 2016,¹⁴⁵ with Twitter reporting a higher figure of 74 per cent compliance out of 24,874 notices received between January and June 2016.¹⁴⁶ Reddit specifically noted in their 2014 report that they receive takedown notifications regarding content that was allegedly defamatory,¹⁴⁷ something that does not generally fall under the purview of copyright law.

This pattern is not solely restricted to the narratives published directly by service providers themselves. One independent study found that around 53 per cent of takedown notifications directed at Google Images over a certain period of time were from a single complainant, and none of them were valid.¹⁴⁸

There are a number of different categories under which abuse of the DMCA can fall. These include attempts to utilise copyright law for non-copyrightable subject-matter, stifling criticism and targeting content that the complainant holds no rights in.¹⁴⁹ In the following sections, some of these examples are explored in more detail.

Trade mark infringement

Inappropriate use of the DMCA as a vehicle to target trade mark infringement is a problem commonly reported by service providers. A specific illustration of this kind of misuse is given in a series of takedown notifications issued by the owners of WhatsApp to the online software development community Github.¹⁵⁰ WhatsApp, a mobile messaging app (which has since been acquired by Facebook¹⁵¹) targeted projects that were merely *related* to the operation of its service, accompanied with the following statement: “there continues to be an extensive amount of content that infringes on WhatsApp Inc.’s copyrights and trademarks”,¹⁵² and that “this continues to cause significant harm to WhatsApp”.¹⁵³

While the DMCA clearly applies to cases involving copyright infringement, it does not provide for trade mark protection.¹⁵⁴ Notably, there is no similar system to the notification and takedown process in place for these disputes.¹⁵⁵ By listing trade mark concerns as part of their takedown notice, WhatsApp appear to have sought the removal of legitimate content either through a misuse of the DMCA notification and takedown process, or by an attempt to “shoe-horn” their claim into its scope.¹⁵⁶ This view is reinforced by the fact that one of the specified, allegedly infringing projects only contained the name WhatsApp, and no other content over which copyright could be claimed.¹⁵⁷

In another example, the photography website DigitalRev received a takedown notification concerning material posted in an article comparing a “Go Pro Hero 3” camera with another available on the market at the time.¹⁵⁸ This in itself would have been problematic, as the author would have a solid fair use defence, given that the material was being used for the purposes of “commentary or criticism”. However, the takedown notification itself contended that the review was infringing the complainant’s trade mark registrations, with no reference to any copyrightable subject-matter included at all.¹⁵⁹ The article was removed at first, only to be restored later, after the takedown was retracted on the basis that it had been an instance of “erroneous enforcement”.¹⁶⁰ In response, DigitalRev highlighted the issue in a follow-up article, claiming that “more than 50% of DMCA notices are filed with an abusive nature to suppress freedom of expression or to prevent fair competitions”.¹⁶¹

Comments left on coverage of the incident afterwards, claiming to be from representatives of GoPro, sought to explain that the notice was sent as DigitalRev was using “incorrect branding and representation of [the] product in their online commerce store”, and that “our letter did not clearly communicate this”.¹⁶² Even if this explanation is authentic, it fails to explain why a DMCA takedown notification was used to address issues with the usage of

¹⁴⁵ “Intellectual Property”, *WordPress.com Transparency Report* (2016), <https://transparency.automattic.com/intellectual-property/2016-h1> [Accessed 14 December 2018].

¹⁴⁶ “Copyright Notices”, *Twitter Transparency Report*, <https://transparency.twitter.com/en/copyright-notices.html> [Accessed 14 December 2018].

¹⁴⁷ See <https://www.reddit.com/wiki/transparency/2014> [Accessed 14 December 2018].

¹⁴⁸ Urban et al., “Notice and Takedown in Everyday Practice” (2017), p.12, para.7.

¹⁴⁹ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 403, para.2.

¹⁵⁰ C. Doctorow, “Whatsapp abused the DMCA to censor related projects from Github” (21 February 2014), *BoingBoing.net*, <http://boingboing.net/2014/02/21/whatsapp-abused-the-dmca-to-ce.html> [Accessed 14 December 2018].

¹⁵¹ D. Rushe, “WhatsApp: Facebook acquires messaging service in \$19bn deal” (20 February 2014), *Guardian Online*, <http://www.theguardian.com/technology/2014/feb/19/facebook-buys-whatsapp-16bn-deal> [Accessed 14 December 2018].

¹⁵² Text of the takedown notice available at <https://github.com/github/dmca/blob/master/2014/2014-02-12-WhatsApp> [Accessed 3 January 2019].

¹⁵³ See <https://github.com/github/dmca/blob/master/2014/2014-02-12-WhatsApp> [Accessed 3 January 2019].

¹⁵⁴ “Frequently Asked Questions (and Answers) about DMCA Safe Harbor”, *Chilling Effects Clearing House*, <https://www.chillingeffects.org/dmca512/faq#QID56> [Accessed 14 December 2014]; and J.R. Brege and K.A. Ovies, “Taking Down Trademark Bullying: Skteching the Contours of a Trademark Notice and Takedown Statute” (2012) 12 *Wake Forest Journal of Business and Intellectual Property Law* 391, 397, para.1.

¹⁵⁵ Brege and Ovies, “Taking Down Trademark Bullying” (2012) 12 *Wake Forest Journal of Business and Intellectual Property Law* 391, 395, para.1.

¹⁵⁶ Brege and Ovies, “Taking Down Trademark Bullying” (2012) 12 *Wake Forest Journal of Business and Intellectual Property Law* 391, 397, para.1.

¹⁵⁷ Rushe, “WhatsApp: Facebook acquires messaging service in \$19bn deal” (20 February 2014), *Guardian Online*, <http://www.theguardian.com/technology/2014/feb/19/facebook-buys-whatsapp-16bn-deal> [Accessed 14 December 2018].

¹⁵⁸ M. Zhang, “GoPro Uses DMCA to Take Down Article Comparing its Camera with Rival” (20 March 2013), *PetaPixel*, <http://petapixel.com/2013/03/20/gopro-uses-dmca-to-take-down-article-comparing-its-camera-with-rival> [Accessed 14 December 2018].

¹⁵⁹ Zhang, “GoPro Uses DMCA to Take Down Article Comparing its Camera with Rival” (20 March 2013), *PetaPixel*, <http://petapixel.com/2013/03/20/gopro-uses-dmca-to-take-down-article-comparing-its-camera-with-rival> [Accessed 14 December 2018].

¹⁶⁰ “GoPro doesn’t like their Hero 3 Compared to Sony’s AS15?” (20 March 2013), *DigitalRev.com*, <https://store.digitalrev.com/article/gopro-doesn-t-like-their/ODUyNjU2ODcA> [Accessed 18 December 2018].

¹⁶¹ See above.

¹⁶² T. Cushing, “Digital Camera Review Taken Down by a Botched DMCA Notice that Makes Claims of Trademark Infringement” (21 March 2013), *TechDirt.com*, <https://www.techdirt.com/articles/20130320/10452722397/digital-camera-review-taken-down-botched-dmca-notice-that-makes-claims-trademark-infringement.shtml> [Accessed 14 December 2018].

trade marks in the first place. Rather than a problem of unclear communication, this is an example of using a completely inappropriate legal process for the situation involved.

Another incident demonstrating the improper use of the DMCA to target alleged trade mark infringement involved an online community based on a fitness regime named “CrossFit”. The organisation in question objected to the use of their trade mark, and submitted takedown notifications to the hosts of the community. Eventually, they sued for trade mark infringement, and the defendant submitted a counter-claim. During the proceedings, CrossFit argued they could have easily submitted an alternative trade mark action to get the disputed content taken down anyway (but didn’t), and so weren’t really abusing the system by making use of the DMCA for that purpose.¹⁶³ The court sensibly disagreed, stating that whether or not CrossFit could have had the material removed by some other means had “no bearing” on whether or not their actions complied with the DMCA.¹⁶⁴ As a result, the possibility of seeking damages under §512(f) was left open to the subscriber, and something that will be returned to in a later section.

The attitude of CrossFit illustrates the seemingly widespread view that the notification and takedown provisions of the DMCA are purely a means to an end, or another tool that can be deployed to remove disagreeable material from the Internet, irrespective of its legal suitability. In these cases, there appears to be remarkably scant regard for due process, so long as the desired result is obtained.

Silencing critics

The above examples illustrate occasions where the DMCA was used inappropriately to target alleged trade mark infringement. In addition to this, there are also numerous examples of where the notification and takedown procedure has been used in an attempt to censor material¹⁶⁵ that is critical of individuals or organisations. This is yet another example that demonstrates how rather than being used for its intended purpose, “copyright has come systematically to stifle criticism”.¹⁶⁶

Perhaps one of the most prominent examples of the DMCA being used as a tool of censorship relates to the controversial Church of Scientology,¹⁶⁷ which has brought numerous lawsuits against parties who have criticised the church and its “foibles” online.¹⁶⁸ This approach to copyright law enforcement has been described as an “attempt to chill free speech on the web”,¹⁶⁹ with the threat of litigation in of itself often enough to prevent others from speaking out, through acts of “self-censorship”.¹⁷⁰

The use of copyright law by the CoS as a weapon against its critics is displayed in the case of *Religious Technology Centre v Netcom On-line Communications Servs Inc*¹⁷¹ that took place before the DMCA’s enactment. Here, the CoS brought actions against a former member who was posting critical materials online, as well as his ISP, and the Bulletin Board Service provider where the discussions were taking place. The court rejected the argument that either the ISP or BBS were liable for direct copyright infringement as a result of actions undertaken by their users.¹⁷² However, they did allow for the possibility that online service providers could be liable either vicariously, or under a theory of contributory infringement in differing circumstances.¹⁷³ It has been opined that it was this potential that helped advance the introduction of the DMCA, in order to address the issue in a statutory form.¹⁷⁴

The notification and takedown procedure of the DMCA, in conjunction with the aggressive attitude of the CoS towards litigation, has been said to have “the most chilling effect” on online freedom of speech.¹⁷⁵ On just one occasion, the CoS sent over 4,000 takedown notifications concerning critical videos posted by an anonymous group to YouTube.¹⁷⁶ Rather than prevent the unauthorised distribution of intellectual property, it appears that the main intention of the CoS in utilising copyright law was to “silence critics and send a warning message to other disgruntled Church members”.¹⁷⁷ This is a prime example that demonstrates the inappropriate use of copyright as a tool for censorship, where “holders too often seek to use their proprietary control of expression to silence the speaker”.¹⁷⁸

The Electronic Frontier Foundation¹⁷⁹ is an American organisation set up to “[defend] civil liberties in the digital world”.¹⁸⁰ Their stated aims are to “ensure that rights and freedoms are enhanced and protected as our use of

¹⁶³ *CrossFit Inc v Alvies*, No.13–3771, 2014 WL 251760 (N.D. Cal. 22 January 2014).

¹⁶⁴ *CrossFit Inc v Alvies*, No.13–3771, 2014 WL 251760 (N.D. Cal. 22 January 2014), p.6, para.1.

¹⁶⁵ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 392, para.2.

¹⁶⁶ Netanel, *Copyright’s Paradox* (2008), p.20, para.1.

¹⁶⁷ CoS.

¹⁶⁸ Netanel, *Copyright’s Paradox* (2008), p.126.

¹⁶⁹ Lyons, “Scientology or Censorship: You Decide”, Camden Rutgers School of Law Publications (2000), p.4 para.1.

¹⁷⁰ Netanel, *Copyright’s Paradox* (2008), p.126.

¹⁷¹ *Religious Technology Center v Netcom On-line Communication Servs, Inc* 923 F. Supp. 1231, 1240 (N.D. Cal. 1995).

¹⁷² *Religious Technology Center v Netcom On-line Communication* 923 F. Supp. 1231, 1382, 1381 (N.D. Cal. 1995).

¹⁷³ *Religious Technology Center v Netcom On-Line Communication* 907 F. Supp. 1231, 1361 (N.D. Cal. 1995).

¹⁷⁴ Lyons, “Scientology or Censorship: You Decide” (2000), p.16, para.1.

¹⁷⁵ Lyons, “Scientology or Censorship: You Decide” (2000), p.18, para.1.

¹⁷⁶ Miller, “Fair Use Through the Lenz of §512(c) of the DMCA” (2010) 95 *Iowa Law Review* 1697, 1708, para.1.

¹⁷⁷ Lyons, “Scientology or Censorship: You Decide” (2000), p.18, para.2.

¹⁷⁸ Netanel, *Copyright’s Paradox* (2008), p.125.

¹⁷⁹ EFF.

¹⁸⁰ See <https://www EFF.org/about> [Accessed 14 December 2018].

technology grows”.¹⁸¹ They have highlighted a number of different abuses of the DMCA process, particularly where it has been misused in an attempt to silence critics. One such instance involved a radio host named Rush Limbaugh. Rush attacked a Georgetown University law student named Sandra Fluke on his show, over a course of three days, for her role in testifying to Congress¹⁸² in support of legislation regarding contraceptives.¹⁸³ The website Daily Kos published a video containing various clips of Rush’s attacks to YouTube.¹⁸⁴ Despite the obvious fair use argument, the material was promptly taken down as the result of a DMCA takedown notification sent to the host.¹⁸⁵ Google later restored the video before the mandated 10–14-day period was up, after the case garnered publicity.

In another example, Uri Geller, a TV psychic famous for claiming an ability to bend spoons with his mind, was subject to a YouTube video looking to expose his supposedly paranormal abilities as fraudulent. The post prompted the issuance of a DMCA takedown notification targeting the entire video. This action was taken despite the content in question only constituting a minor portion of the larger work, which would have made for a compelling fair use argument when considering its critical purpose. The EFF filed a complaint on behalf of the individual who uploaded the video, seeking damages under §512(f).¹⁸⁶ The case was eventually settled out of court, with part of the settlement including a requirement that the material in question be licensed under the Creative Commons, allowing for it to be re-used in future by anybody for non-commercial purposes.¹⁸⁷

In 2007, a video blogger named Michelle Malkin posted a video criticising the behaviour of the artist Akon. The video included clips of the artist’s live performances, with Malkin condemning what she described as his “misogyny”.¹⁸⁸ Akon’s record label, Universal Music Group¹⁸⁹ issued a takedown notification regarding the video, which led to YouTube disabling access to it to give effect to the DMCA. After Malkin contacted the EFF for assistance,¹⁹⁰ a counter-notice was filed, on the basis that

the material fell under fair use protections. After this, it was restored without any further legal action being taken.¹⁹¹ This again demonstrated an abuse of the system for the purposes of censorship, as the subject matter involved was not copyrightable material.¹⁹²

In another instance, the NFL used the DMCA to target a video posted online that was critical of its copyright policy, and “almost certainly illegitimate”.¹⁹³ They then found that access was later restored upon the receipt of a valid counter-notification. Instead of following the correct process, which would be to initiate legal proceedings against the subscriber, the NFL sent another takedown notification concerning the same material.¹⁹⁴ Not only does this demonstrate an abuse of the takedown process to censor legitimate criticism, but also a lack of respect more generally for the “procedural sanctity” of the DMCA itself.¹⁹⁵

Continuing on in the same vein, the Ralph Lauren fashion label came under fire after one of its adverts appeared to be digitally manipulated to such an extent that the model’s head was wider than her waist. The criticisms were published on a number of websites, including the online community and publishing site *boingboing.net*, which subsequently received a DMCA takedown notice via its host. With support from Wendy Seltzer of the Chilling Effects Clearinghouse project,¹⁹⁶ Boing Boing refused to take down the content, challenging Ralph Lauren to “sue and be damned”, relying on fair use protections for their criticism of the actions. No further action was taken,¹⁹⁷ but this instance again demonstrates the abuse of the DMCA to stifle criticism, rather than to protect legitimate copyright concerns.

In another incident, the price list for the fees charged to law enforcement agencies by the service provider Yahoo for compliance with requests for user information was published in 2009 on a site called Cryptome.org. Unhappy about the material’s distribution, and concerned about the potential negative press the release would garner, Yahoo sent a DMCA takedown notification to

¹⁸¹ See <https://www.eff.org/about> [Accessed 14 December 2018].

¹⁸² See her opening statement on YouTube: <https://www.YouTube.com/watch?v=xIRCOnsjtKQ> [Accessed 14 December 2018].

¹⁸³ M. Zimmerman, “Limbaugh Copies Michael Savage’s Bogus Copyright Theory, Sends DMCA to Silence Critics” (24 April 2012), *Electronic Frontier Foundation*, <https://www.eff.org/deeplinks/2012/04/limbaugh-copies-michael-savages-bogus-copyright-theory> [Accessed 14 December 2018].

¹⁸⁴ “53 of Rush Limbaugh’s most vile smears against Georgetown Law student Sandra Fluke” (5 March 2012), *YouTube*, <https://www.YouTube.com/watch?v=q1oOjKQfIN0> [Accessed 14 December 2018].

¹⁸⁵ “Rush Limbaugh demands YouTube remove *Daily Kos* video... watch it here” (23 April 2012), *Daily Kos*, <http://www.dailykos.com/story/2012/04/23/1085791/-Rush-Limbaugh-demands-YouTube-remove-Daily-Kos-video-watch-it-here> [Accessed 14 December 2018].

¹⁸⁶ “Sapient v. Geller Complaint”, *Electronic Frontier Foundation*, <https://www.eff.org/document/complaint-25> [Accessed 14 December 2018].

¹⁸⁷ “Sapient v. Geller”, *Electronic Frontier Foundation*, <https://www.eff.org/cases/sapient-v-geller> [Accessed 14 December 2018].

¹⁸⁸ “Malkin Fights Back Against Copyright Law Misuse by Universal Music Group” (9 May 2007), *Electronic Frontier Foundation*, <https://www.eff.org/deeplinks/2007/05/malkin-fights-back-against-copyright-law-misuse-universal-music-group> [Accessed 14 December 2018].

¹⁸⁹ UMG.

¹⁹⁰ M. Malkin, “Akon’s record company abuses DMCA to stifle criticism on YouTube” (3 May 2007), <http://michellemalkin.com/2007/05/03/akons-record-company-abuses-dmca-to-stifle-criticism-on-youtube> [Accessed 14 December 2018].

¹⁹¹ M. Malkin, “UMG & YouTube retreat over Akon report” (14 May 2007), <http://michellemalkin.com/2007/05/14/umg-youtube-retreat-over-akon-report> [Accessed 14 December 2018].

¹⁹² Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 392, para.2.

¹⁹³ Sundell, “Tempting the Sword of Damocles” (2011) 12 Minn. Journal of Law, Science, and Technology 335, 347, para.2.

¹⁹⁴ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 396.

¹⁹⁵ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 396, para.3.

¹⁹⁶ Now known as the “Lumen Database”.

¹⁹⁷ C. Doctorow, “The criticism that Ralph Lauren doesn’t want you to see!” (6 October 2009), *BoingBoing.net*, <http://boingboing.net/2009/10/06/the-criticism-that-r.html> [Accessed 14 December 2018].

Cryptome in an attempt to have it taken offline. Cryptome refused to comply,¹⁹⁸ and the material was still online as of December 2018.¹⁹⁹

The majority of the preceding examples have illustrated situations where the DMCA has been abused in order to have content removed inappropriately where the complainant has had an intellectual property interest in the material, yet the use was clearly non-infringing. Another way in which the DMCA is abused is through the erroneous submission of takedown notifications where the complainant holds no rights to that over which they are claiming alleged copyright infringement. This is something that was also demonstrated in the *Viacom v YouTube* case introduced earlier, where the plaintiff submitted numerous takedown notifications that referred to material in which they held no intellectual property rights.²⁰⁰ This was described by the actual owners of the works as a “blatant abuse” of the DMCA system as part of the defendant’s response to the action.²⁰¹

The late artist Prince was known to be involved in a number of dubious copyright disputes. This was to such an extent that the EFF have included him in their “Takedown Hall of Shame”,²⁰² a section of their website used to highlight “the worst of the worst” in terms of “bogus” copyright complaints. One of these instances involved fan-shot videos from a performance by Prince at the Coachella festival. The videos in question showed the artist performing a cover of the song “Creep” by the British band Radiohead. After being uploaded to YouTube, Prince’s record label sought to have them removed, as they were allegedly infringing copyright.²⁰³ While Prince had some rights as an artist in the distribution of the performance itself, commentators have pointed out that there was no copyright infringement in these circumstances that should have been remedied with the use of a DMCA takedown notice.²⁰⁴

Examples of erroneous takedowns are plentiful, and one just needs to spend some time looking through Google’s transparency report to discover some unexpected statistics, such as the six takedown notifications that were sent to Google relating to alleged copyright infringement on *whitehouse.gov*,²⁰⁵ the 23 takedowns targeting *justice*

.gov,²⁰⁶ or the 14 aimed at *nasa.gov*,²⁰⁷ none of which are locations known for hosting pirated material. Perhaps wisely, Google reported that they removed search engine listings in response to zero of these particular requests.

Automated takedown notifications

In order to deal with the onerous task of scouring the web for unauthorised instances of copyrighted material, right holders increasingly outsource the work to dedicated third parties.²⁰⁸ These organisations often employ automated means to detect content, and then send out DMCA takedown notifications en masse.²⁰⁹ One such organisation is MarkMonitor, who have described themselves as a “leading brand protection provider”.²¹⁰ Technology is deployed to search the Internet for the client’s brands or products, which then sends takedown notifications to the hosts of the allegedly infringing content.²¹¹ This sort of automated approach is cost-effective for copyright holders, who do not have to dedicate significant resources towards the task of online revenue protection. However, the nature of the system means that it is imperfect, leading to material being inaccurately identified as infringing, and thus becoming the subject of an inaccurate takedown notification. This is an unsurprising eventuality, because as we have already seen in the examples up to this point, the DMCA has fostered “an environment that rewards indiscriminate, hair-trigger takedown requests”.²¹² “Spray and pray” can often provide far more substantial results in terms of takedown volume than careful and targeted notifications.

Right holders claim that there is human involvement in the automated processes to avoid mistakes,²¹³ but in practice it is clear that they still happen. In just one study, about 4 per cent of notices were found to identify work that was different from that which they were claiming copyright over in the first place,²¹⁴ thus targeting unrelated material for takedown. Over 13 per cent of notices in the same study did not provide adequate information to identify the allegedly infringing work, often because the

¹⁹⁸ F.V. Lohmann, “Latest Bogus DMCA Takedown Award Winner: Yahoo!” (7 December 2009), *Electronic Frontier Foundation*, <https://www.eff.org/deeplinks/2009/12/todays-bogus-dmca-takedown-award-winner-yahoo> [Accessed 14 December 2018].

¹⁹⁹ “Yahoo! Compliance Guide for Law Enforcement”, *Cryptome.org*, <http://cryptome.org/isp-spy/yahoo-spy.pdf> [Accessed 14 December 2018].

²⁰⁰ Hassanabadi, “Viacom v. YouTube – All Eyes Blind: The Limits of the DMCA in a Web 2.0 World”, (2011) 26 *Berkeley Technology Law Journal*, p.437, para.3; and Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 *Minn. Journal of Law, Science, and Technology* 387, 398, para.2.

²⁰¹ Hassanabadi, “Viacom v. YouTube – All Eyes Blind: The Limits of the DMCA in a Web 2.0 World”, (2011) 26 *Berkeley Technology Law Journal*, p.438 para.1; and Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 *Minn. Journal of Law, Science, and Technology* 387, 398, para.2.

²⁰² “Takedown Hall of Shame”, *Electronic Frontier Foundation*, <https://www.eff.org/takedowns> [Accessed 14 December 2018].

²⁰³ H. d’Andrade, “Prince Issues One Takedown Too Many” (2 June 2008), *Electronic Frontier Foundation*, <https://www.eff.org/deeplinks/2008/06/prince-issues-one-takedown-too-many> [Accessed 4 October 2018].

²⁰⁴ D’Andrade, “Prince Issues One Takedown Too Many” (2 June 2008), *Electronic Frontier Foundation*, <https://www.eff.org/deeplinks/2008/06/prince-issues-one-takedown-too-many> [Accessed 14 December 2018]; and S. Bayard, “Prince, Radiohead, and the Bootlegging Provision of the Copyright Act” (2 June 2008), *Digital Media Law Project*, <http://www.dmlp.org/blog/2008/prince-radiohead-and-bootlegging-provision-copyright-act> [Accessed 14 December 2018].

²⁰⁵ See <https://www.google.com/transparencyreport/removals/copyright/searchdata/domains/?id=whitehouse.gov> [Accessed 14 December 2018].

²⁰⁶ See <https://www.google.com/transparencyreport/removals/copyright/searchdata/domains/?id=justice.gov> [Accessed 14 December 2018].

²⁰⁷ See <https://www.google.com/transparencyreport/removals/copyright/searchdata/domains/?id=nasa.gov> [Accessed 14 December 2018].

²⁰⁸ Urban et al., “Notice and Takedown in Everyday Practice” (2017), p.2, para.6.

²⁰⁹ Neill and Lee, “Fixing Section 512” (2016) *American Intellectual Property Law Association Quarterly Journal*, para.1, available at <https://ssrn.com/abstract=2879696> [Accessed 14 December 2018].

²¹⁰ See <https://www.markmonitor.com/why-markmonitor/the-leader-in-brand-protection-and-domain-management?cid=homepage> [Accessed 14 December 2018].

²¹¹ “Datasheet: MarkMonitor AntiPiracy” (undated), https://www.markmonitor.com/download/ds/ds-MarkMonitor_AntiPiracy.pdf [Accessed 14 December 2018].

²¹² Sundell, “Tempting the Sword of Damocles” (2011) 12 *Minn. Journal of Law, Science, and Technology* 335, 346, para.2.

²¹³ Urban et al., “Notice and Takedown in Everyday Practice” (2017), p.35, para.3.

²¹⁴ Urban et al., “Notice and Takedown in Everyday Practice” (2017), p.90, para.3.

URLs in question related to a dynamic search or “category” style page.²¹⁵ These issues are the hallmarks of automated takedowns.

One of the most potentially embarrassing scenarios for a copyright holder is where the agent that they have enlisted to track down unauthorised uses of their intellectual property mistakenly targets the official source itself. This exact scenario was illustrated in a takedown notification issued by the third-party agent DtecNet (part of MarkMonitor) to Google on behalf of the American media organisation HBO. In the notification, a large number of URLs were listed as allegedly infringing HBO’s copyrights, including those on HBO’s own website.²¹⁶ Not only that, the takedown notification also listed other prominent media sources such as MTV’s Movie blog, and *IGN.com*—both of which contained reviews of the HBO film *Eastbound & Down*, and no pirated links.²¹⁷ Another example of this kind came again in the form of takedown notifications issued by DtecNet, but this time on behalf of Fox. Seeking to target the unauthorised distribution of their TV show *Homeland*, the takedowns named not just sources of piracy, but also managed to target the novel of the same name by Cory Doctorow, which was available under a Creative Commons licence.²¹⁸ Finally, the RIAA sent takedown notifications targeting content on websites operated by parties that they themselves had employed to promote the music of their members.²¹⁹

This particular issue is one that comes up time and again, with one such example dubbed by TorrentFreak as the “the world’s most idiotic copyright complaint”.²²⁰ In it, a takedown notification was submitted to Google from the Total Wipes Music Group, reportedly targeting the unauthorised distribution of various albums to which they held copyrights. However, stating that “We have an exclusive & worldwide deal for distributing this content”, they specified a list of 95 URLs, which included the download pages for a host of different kinds of software such as Skype, Joomla, Evernote, Ubuntu and Open Office²²¹—in none of which Total Wipes had any intellectual property rights. This was just one example out of a number of takedown notifications where the group incorrectly identified material as infringing,²²² and in a statement to the online publication ARSTechnica, they blamed a technical glitch:

“Taking a look at [the url, it] is pretty clear that for a few hours only the word ‘download’ has been used by the script and that caused several illegal and wrong DMCA request [*sic*].”²²³

Aside from the obvious abuse of the DMCA here, and the resulting impact on the legitimate copyright holders who had their content removed, this sort of misidentification has other implications, in that it is particularly problematic given the legal nature of the takedown process. Ultimately, the signatory is stating under penalty of perjury that the individual notices sent out are accurate—whether or not they are checked manually beforehand. As a result, any failures in the detection technology could result in unexpected liability. It was hoped that the inclusion of a statement that the complainant had considered the fair use potential before sending the takedown notification would help give pause, and prevent the use of automated detection and reporting systems.²²⁴ However, even after the effective implementation of this requirement as the result of *Lenz*, there appears to have been no real reduction in the volume of takedown notices reported by major online service providers in their transparency reports. This should come as no real surprise, as it is difficult to see why companies who were already content to sign off on bulk takedown notifications being sent out in their name “under penalty of perjury” would be deterred by the added requirement to say they had considered fair use, which is still determined by a subjective, rather than objective test.²²⁵

An additional problem with third-party services whose businesses are built on the notification and takedown system is that they have a vested interest in producing results—whether or not the takedown is strictly within the terms of the statute. Until early 2017, one such agent (DMCA.com) explicitly stated the following on their homepage: “We get stolen content removed. It’s 100% guaranteed – or you get your money back.”²²⁶ As well as issuing takedown notices regarding material that was created by a client, they also claimed to work with “stolen content” such as pictures and videos where the complainant was the *subject*.²²⁷ Usually, the rights in a

²¹⁵ Urban et al., “Notice and Takedown in Everyday Practice” (2017), p.93, para.5.

²¹⁶ “DtecNet DMCA (Copyright) Complaint to Google” (19 December 2012), <https://lumendatabase.org/notices/652104> [Accessed 14 December 2018].

²¹⁷ See above.

²¹⁸ M. Masnick, “Fox Uses Bogus DMCA Claims to Censor Cory Doctorow’s Book About Censorship” (22 April 2013), <https://www.techdirt.com/articles/20130421/14043222791/fox-uses-bogus-dmca-claims-to-censor-cory-doctorows-book-about-censorship.shtml> [Accessed 14 December 2018].

²¹⁹ J. M. Miller, “Fair Use Through the Lenz of §512(c) of the DMCA: A Preemptive Defense to a Premature Remedy?” (2010) *Iowa Law Review*, pp.1725-1726.

²²⁰ “The World’s Most Idiotic Copyright Complaint”, (22 February 2015), *TorrentFreak*, <https://torrentfreak.com/the-worlds-most-idiotic-copyright-complaint-150222> [Accessed 14 December 2018].

²²¹ “DMCA (copyright) Complaint to Google”, (5 February 2015), *ChillingEffects*, <https://lumendatabase.org/notices/10416081> [Accessed 14 December 2018].

²²² D. Kravets, “‘Bug’ causes music group to bombard Google with bogus DMCA takedowns” (23 February 2015), <http://arstechnica.com/tech-policy/2015/02/bug-causes-music-group-to-bombard-google-with-bogus-dmca-takedowns> [Accessed 14 December 2018].

²²³ Kravets, “‘Bug’ causes music group to bombard Google with bogus DMCA takedowns” (23 February 2015), <http://arstechnica.com/tech-policy/2015/02/bug-causes-music-group-to-bombard-google-with-bogus-dmca-takedowns> [Accessed 14 December 2018].

²²⁴ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 *Minn. Journal of Law, Science, and Technology* 387, 410, para.2.

²²⁵ Neill and Lee, “Fixing Section 512” (2016) *American Intellectual Property Law Association Quarterly Journal*, p.4 paras 1–2 available at <https://ssrn.com/abstract=2879696> [Accessed 14 December 2018].

²²⁶ See <http://www.dmca.com> [Accessed 14 December 2018].

²²⁷ See <http://www.dmca.com/Takedowns.aspx> [Accessed 14 December 2018], and <http://www.dmca.com/FAQ/How-do-I-get-my-picture-taken-off-the-internet> [Last accessed 17 January 2017].

photograph or video lie with the creator,²²⁸ unless they have been acquiesced through contractual agreement. As a result, this guarantee seems misleading, or disingenuous at best. In addition, any attempt to use the DMCA to remove photographs where the complainant did not hold a copyright in could potentially give rise to liability under §512(f)—something that will be discussed in greater detail in an upcoming section.

Response by online service providers to abuse

Online service providers have expressed concern at the levels of takedown notifications they receive that abuse the DMCA provisions,²²⁹ which require a significant and disproportionate amount of resources to deal with effectively,²³⁰ as opposed to the time spent on otherwise legitimate notices. These concerns have led to discussions in the American House of Representatives, with hearings taking place regarding the failings of the DMCA coming before a subcommittee of the Committee on the Judiciary in March 2014.²³¹ In a submitted amicus brief, the interested parties contend that “unfounded DMCA takedown notices are common, and impose a burden on both online service providers and the free exchange of ideas”.²³² They argue that in order to protect their users and push back against abusive or fraudulent uses of the DMCA, online service providers are required to devote significant resources to the cause, harming the development of their business, by not being able to use those elsewhere.²³³ In addition, the amici also expressed concern about the negative effect of fraudulent or abusive DMCA takedown notices on copyright holders who have legitimate complaints, as the time taken to respond to their requests is increased.²³⁴

Paul Sieminski, General Counsel of Automattic, gave testimony on the sorts of abuse of the DMCA that they had come across as part of their daily operations. He referenced an earlier amicus brief that Automattic had participated in, where they had again highlighted abuses of the DMCA.²³⁵ In it, they claimed to regularly receive takedown notices that “[appear] motivated not by an interest in protecting copyright but a desire to improperly silence critics”. One of the specific examples given was the improper use of the DMCA takedown process to target

unauthorised uses of a company’s name or logo on sites that are critical of their business practices—something that falls under fair use protections.²³⁶ Another example given was that of a medical company who published fake customer testimonials on their website, and then submitted a takedown notification to have screenshots on a blog highlighting the practice removed.²³⁷

Tumblr also provided a number of examples of takedown notifications in the amicus brief which they considered to be “baseless and intended to silence lawful speech”.²³⁸ One of these concerned a doctor, who submitted fraudulent takedown notifications posing as the right holder in order to have critical material about his practices removed.²³⁹ Another concerned a model, who tried to use the DMCA to have photographs of her taken offline, despite the intellectual property rights lying with the photographer rather than her.²⁴⁰ There was even an example where a well-known American politician submitted a takedown notice regarding photographs of himself used on a satirical website, even though they were taken by an individual with no relation or association to him, and therefore he did not hold any copyright.²⁴¹

Remedies against DMCA abuse

Abuse of the DMCA did not go without consideration by the statute’s drafters, with remedies to help combat abuse of the notice and takedown process explicitly provided for in the DMCA, under §512(f). It reads:

“Any person who knowingly materially misrepresents ... that material or activity is infringing, or that material or activity was removed or disabled by mistake or misidentification, shall be liable for any damages, including costs and attorneys’ fees, incurred.”²⁴²

This means that the party subject to a fraudulent DMCA takedown notice, as well as the online service provider, can file for damages occurring as the result of material that has been removed.

The first judgment in this area came in the important case of *Online Policy Group v Diebold*.²⁴³ The facts concerned the publication of emails discussing known issues with electronic voting equipment, of which Diebold was the manufacturer. Two students from Swarthmore

²²⁸ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 394, para.3.

²²⁹ Urban et al., “Notice and Takedown in Everyday Practice” (2017), p.40, para.3.

²³⁰ Urban et al., “Notice and Takedown in Everyday Practice” (2017), p.40, para.2.

²³¹ M. Masnick, “If We’re Going to Change DMCA’s ‘Notice and Takedown’, Let’s Focus on How Widely It’s Abused” (14 March 2014), *TechDirt*, <https://www.techdirt.com/articles/20140314/11350426579/if-were-going-to-change-dmcas-notice-takedown-lets-focus-how-widely-its-abused.shtml> [Accessed 14 December 2018].

²³² See *Amicus Brief*, p.6, para.2, https://www.eff.org/files/2013/12/13/osp_lenz_amicus_brief.pdf [Accessed 14 December 2018].

²³³ See *Amicus Brief*, p.10, para.1, https://www.eff.org/files/2013/12/13/osp_lenz_amicus_brief.pdf [Accessed 14 December 2018].

²³⁴ See *Amicus Brief*, p.10, para.1, https://www.eff.org/files/2013/12/13/osp_lenz_amicus_brief.pdf [Accessed 14 December 2018].

²³⁵ See *Amicus Brief*, https://www.eff.org/files/2013/12/13/osp_lenz_amicus_brief.pdf [Accessed 14 December 2018].

²³⁶ See *Amicus Brief*, p.13, para.1, https://www.eff.org/files/2013/12/13/osp_lenz_amicus_brief.pdf [Accessed 14 December 2018].

²³⁷ Testimony of Paul Sieminski (13 March 2014), p.3, <https://judiciary.house.gov/wp-content/uploads/2016/02/031314-Testimony-Sieminski.pdf> [Accessed 14 December 2018].

²³⁸ See *Amicus Brief*, p.17, para.1, https://www.eff.org/files/2013/12/13/osp_lenz_amicus_brief.pdf [Accessed 14 December 2018].

²³⁹ See *Amicus Brief*, p.17, para.3, https://www.eff.org/files/2013/12/13/osp_lenz_amicus_brief.pdf [Accessed 14 December 2018].

²⁴⁰ See *Amicus Brief*, p.17, para.4, https://www.eff.org/files/2013/12/13/osp_lenz_amicus_brief.pdf [Accessed 14 December 2018].

²⁴¹ See *Amicus Brief*, p.17, para.6, https://www.eff.org/files/2013/12/13/osp_lenz_amicus_brief.pdf [Accessed 14 December 2018].

²⁴² DMCA §512(f).

²⁴³ *Online Policy Group v Diebold*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004).

College posted these conversations online, which were then linked to from the independent news organisation IndyMedia's website. Diebold issued a takedown notice under the DMCA to the Online Policy Group,²⁴⁴ who was acting as IndyMedia's webhost. As the subject of the notice was links, and therefore not content that they directly hosted, OPG refused to disable access, and instead sued Diebold, along with the college students. The EFF, along with the Center for Internet and Society Cyberlaw Clinic from Stanford Law, took up the representation, and filed for damages under §512(f). Their argument was that Diebold had "knowingly materially misrepresented" that the material or activity that they were claiming copyright over was infringing. Diebold lost the case, and reportedly went on to agree to damages of \$125,000.²⁴⁵

In delivering the decision, the judge stated that "no reasonable copyright holder" would have thought that the email discussions were subject to copyright protections. He went on to say:

"The fact that Diebold never actually brought suit against any alleged infringer suggests strongly that Diebold sought to use the DMCA's safe harbor provisions – which were designed to protect ISPs, not copyright holders – as a sword to suppress publication of embarrassing content rather than as a shield to protect its intellectual property."²⁴⁶

The judge's comments are fascinating for a number of different reasons. First, it suggests that if a copyright holder only uses the notice and takedown process, and does not then proceed to take action against infringing parties, that it could be inferred that they do not in fact take the alleged infringement seriously. If this is so, then it suggests that the DMCA is only to be treated as a temporary stopgap measure to have content removed while legal proceedings are being prepared – rather than a solution in itself.

In November of 2013, Automattic announced that it intended to take action on behalf of its users in two cases where they believed that the DMCA process was being abused to censor the contents of blogs on their platform.²⁴⁷ In one of the cases,²⁴⁸ the facts concerned a student journalist named Oliver Hotham who published an email interview with a group called "Straight Pride UK" on his WordPress.com site. Unhappy with the way in which

their organisation was portrayed, Straight Pride submitted a DMCA takedown notification, and the allegedly infringing material was removed. The court held that this resulted in a misrepresentation by the complainant, as they "could not have reasonably believed" that it was protected by copyright.²⁴⁹ As the defendant failed to plead, a default judgment was given, with a total of \$25,084 awarded in damages.²⁵⁰ This was an important victory, but may prove to be largely symbolic, owing to the difficulty involved in collecting on the award from an overseas defendant.

Aside from the cases above, there are few examples available of successful claims brought under §512(f) for abuse of the takedown process. The bar is set high, and as a result, it is "exceedingly difficult for an end-user to succeed in a claim for misrepresentation against a copyright holder".²⁵¹ As a result, there is a lack of real consequences for abuse of the DMCA.²⁵² Even where such actions are victorious, there can be difficulties with collecting the damages awarded. Anybody can submit a DMCA takedown notification, and where the complainants is located outside America, it can prove extremely difficult to enforce against them any judgments made under §512(f).

Another issue with the §512(f) remedy is that in order for there to be damages, access to the material in question must actually have been removed, or had access to it disabled.²⁵³ This means that actions can only be brought against parties who abuse the system where the receiving service provider actually processes the takedown notifications. As a result, there are few remedies against those actors who frequently submit fraudulent or abusive takedown notifications that are rebuffed.

Improving the DMCA

It seems clear that the notification and takedown process has "evolved into a highly complex ecosystem",²⁵⁴ and the many criticisms reinforce the view that the DMCA "slipping into irrelevancy".²⁵⁵ With many platforms stressing their reliance on the safe harbour in order to maintain their economic operations,²⁵⁶ it seems likely that without specific intervention, this abuse will continue unabated.²⁵⁷ Significant change will undoubtedly prove a challenge, as running contrary to the commonly perceived copyright narrative of intermediaries versus rights holders,

²⁴⁴ OPG.

²⁴⁵ See <https://www.eff.org/cases/online-policy-group-v-diebold> [Accessed 14 December 2018].

²⁴⁶ *Online Policy Group v Diebold* 337 F. Supp. 2d 1195, 1205 (N.D. Cal. 2004).

²⁴⁷ P. Sieminski, "Striking Back Against Censorship" (21 November 2013), *WordPress.com News*, <http://en.blog.wordpress.com/2013/11/21/striking-back-against-censorship> [Accessed 14 December 2018].

²⁴⁸ *Automattic Inc v Steiner* 82 F. Supp. 3d 1011, 1030, 1032 (N.D. Cal. 2015).

²⁴⁹ *Automattic Inc v Steiner* 82 F. Supp. 3d 1011, 1030, 1032 (N.D. Cal. 2015) at *10.

²⁵⁰ *Automattic Inc v Steiner* 82 F. Supp. 3d 1011, 1030, 1032 (N.D. Cal. 2015) at Part IV. See <https://docs.justia.com/cases/federal/district-courts/california/candce/4-2013cv05413/272130/37> [Accessed 14 December 2018].

²⁵¹ O'Donnell, "Lenz v. Universal Music Corp. and the Potential Effect of Fair Use Analysis Under the Takedown Procedures of §512 of the DMCA" (2009) 10 *Duke Law & Technology Review*, available at <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1194&context=dltr> [Accessed 3 January 2019].

²⁵² Cobia, "The Digital Millennium Copyright Act Takedown Notice Procedure" (2009) 10 *Minn. Journal of Law, Science, and Technology* 387, 394, para.2.

²⁵³ USC 17 §512(f)(2).

²⁵⁴ Urban et al., "Notice and Takedown in Everyday Practice" (2017), p.3 para.2.

²⁵⁵ Hassanabadi, "Viacom v. YouTube – All Eyes Blind: The Limits of the DMCA in a Web 2.0 World", (2011) 26 *Berkeley Technology Law Journal*, p.405 para 1.

²⁵⁶ Urban et al., "Notice and Takedown in Everyday Practice" (2017), p.114, para.2.

²⁵⁷ Miller, "Fair Use Through the Lenz of §512(c) of the DMCA" (2010) 95 *Iowa Law Review* 1697, 1723, para.4.

the two groups “are not monolithic”,²⁵⁸ with substantial nuance involved. With that caution in mind, there remain a number of different proposals that would help address the issues with §512 that have been outlined. Some of these are introduced and analysed below.

Procedural clarification and amendment

The most obvious starting point for the improvement of the notification and takedown process is perhaps in its statutory requirements. Simple amendments to address the open questions outlined earlier in this paper would help bring clarity, and reduce a reliance on the interpretation and policy decisions of individual intermediaries.

Another major area of improvement would be to take steps to address the disparity between the formal requirements of a takedown versus a counter-notification. To achieve this, both parties should be allowed to act through a designated third-party agent, rather than this avenue being open solely to the original complainant. In addition, the 10- to 14-day period that must pass after a counter-notification has been received before access to allegedly infringing material can be restored by a service provider should also be shortened, or done away with altogether. This would reduce the immediate harmful impact of fraudulent or abusive takedown notifications, by allowing access to the content to be quickly reinstated. Given that the subscriber is stating that they have the right to use the content as part of the counter notification process—there appears to be little requirement for this interstitial buffer.

Secondly, our understanding of copyright must be reshaped in light of how we now culturally engage with material. There should be explicit exceptions under the DMCA for material that is reproduced without seeking any commercial gain, and used merely as cultural reference.²⁵⁹

Penalties for abuse

It is clear that there are no real practical penalties for those that submit notices in bad faith that may otherwise be considered formally valid.²⁶⁰ To help deter abuse of the DMCA, one approach would be for those who repeatedly submit fraudulent or abusive takedown notifications to be subject to the same kind of repeat infringer policy that applies to those who consistently infringe copyrights. This could be done through a temporary suspension of their privilege to submit takedown notifications, or in extreme cases, even by suspending their copyright enforcement rights entirely for a temporary basis.²⁶¹ This

is something that at least one online service provider has elected to pursue unilaterally, with “The Ultimate Ebook Library” threatening to ignore all future takedown notifications from a particular complainant who they considered to have repeatedly abused the process.²⁶² However, this is a risky strategy, as without statutory backing, the platform would lose its safe harbour protections, and risks opening itself up to future liability from legitimate copyright claims that are not acted upon, even if they originate from a serial DMCA abuser.

Deeper involvement of the US Copyright Office

Writing in 2009, Jeffrey Cobia put forward the suggestion that in order to combat DMCA abuse, an additional branch of the US Copyright Office could be created which would conduct an initial investigation into all DMCA takedown notifications.²⁶³ This would help ensure that the implications for freedom of speech and fair use were given due consideration. Cobia argued that while there may be a backlog initially, that copyrights should also be required to be formally registered in order to receive protection. This would help reduce the complexity of the cases, as well as the training required to deal with them,²⁶⁴ and such a revised system would see a reduction in fraudulent and arbitrary claims over time.²⁶⁵ However, it is difficult to see how this would operate in practice today.

A requirement for all copyrights to be registered with the US Copyright Office would effectively mean that any time anybody took a photograph, or wrote a blog post, or recorded a video on their phone, they would need to go through a formal registration process in order to ensure that their rights were protected from unauthorised dissemination and reproduction. As well as creating an undue burden on right holders as a result, it would also place immense pressure on the USCO as a central repository. The registration requirement may make sense to some extent in a commercial setting, but not in the world of instant authorship and content publication. Another question that would need to be considered would be the overall role of the DMCA, which has become the de facto process for many international complaints to have content taken down online, thanks to the dominance of the American technology sector.

If there were practical solutions to the problems posed by a focus on registration, it remains difficult to see how any single agency could cope with the vast quantities of takedown notifications that are currently handled by online service providers, many of whom currently do not have a manual review process. Google alone has received billions of takedown notices, affecting over one million

²⁵⁸ Urban et al., “Notice and Takedown in Everyday Practice” (2017), p.4, para.3.

²⁵⁹ Sundell, “Tempting the Sword of Damocles” (2011) 12 Minn. Journal of Law, Science, and Technology 335, 350, para.2.

²⁶⁰ Urban et al., “Notice and Takedown in Everyday Practice” (2017), p.117, para.1.

²⁶¹ Sundell, “Tempting the Sword of Damocles” (2011) 12 Minn. Journal of Law, Science, and Technology 335, p. 1725–1726.

²⁶² “Ebook Library Punishes Anti-Piracy Outfit for Wrongful DMCA Notices” (11 March 2015), *TorrentFreak.com*, <https://torrentfreak.com/ebook-library-punishes-anti-piracy-outfit-for-wrongful-dmca-notices-150311/> [Accessed 14 December 2018].

²⁶³ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 404–405.

²⁶⁴ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 405, para.1.

²⁶⁵ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 405, para.3.

separate websites from March 2011 to February 2017.²⁶⁶ Clearly, sweeping changes would need to be made to core parts of the DMCA to reduce this kind of volume substantially in order for any single agency to handle it. One such step would be to outlaw the use of automated bots to send out takedown notifications, though that would be incredibly problematic to detect or to enforce in practice. It seems that the costs involved in the creation of such a department would indeed be prohibitive.

Finances aside, another significant issue with the proposal would concern the time taken to process requests. One of the main benefits of the DMCA for copyright holders is the ability to have access to allegedly infringing content removed rapidly, without the need for the involvement of a third party to make that determination. Even if response times were relatively low, including the USCO as a first call for every single takedown notification would inevitably add to the time involved.

Finally, establishing a branch within the USCO with the aim of rejecting takedown notifications that target fair use of material would effectively turn that branch into a court of first instance. As outlined earlier, the fair use doctrine is highly dependent on the facts of each situation, and depends on judicial interpretation for its application. It is often far from certain which way a case will go, even if there is a solid fair use argument. It seems inevitable that pursuing this approach as a solution would instead result in increased litigation, in order to overturn the initial decisions of the USCO.

It seems clear that the absence of any real negative fallout from abuse of the DMCA means that the notification and takedown process is simply viewed as another tool in the arsenal of “content bullies”²⁶⁷ to have material they dislike taken offline, irrespective of its legality, and so perhaps the most effective change to help prevent abuse of the DMCA would simply be to take steps ensure that there are real consequences for those who misuse the system,²⁶⁸ as “a penalty of perjury that does not include a tangible consequence is not an effective deterrent”.²⁶⁹ The current scope for damages under §512(f) is inadequate, and ineffective, with much resting on poorly defined ideas of what constitutes fair use.²⁷⁰ In order to ensure consistency within the law, the doctrine of fair use should be more tightly defined, rather than operating on the particular facts involved.²⁷¹ This would have the dual benefit of reducing fraudulent submissions,

while also providing subscribers with clear guidelines on what use was and was not permissible.²⁷² There have been specific suggestions made with regard to how the above may be achieved, including the alteration of the statutory language to more explicitly spell out who would be eligible to claim damages, for what, and in what circumstances,²⁷³ so this is not an aim which would be practically impossible to achieve.

These examples demonstrate just some of the possible changes that could be adopted to help curtail abuse of the DMCA, and address the procedural idiosyncrasies that result in imbalance. Whatever path is ultimately taken, it is unlikely to happen quickly, with intellectual property right holders arguing that online service providers should be doing more to ensure that their platforms are not repeatedly used for hosting infringing content through a “notice and staydown” system²⁷⁴ and the platforms themselves pushing for more to be done about the indiscriminate use of the DMCA for inappropriate reasons.

Summary

The compromise reached in the DMCA notification and takedown process between the interests of copyright holders, online service providers, and protecting freedom of speech has now existed for 20 years, throughout the formative years of today’s digital economy. It has successfully protected technology firms from liability—helping ensure their exponential growth and economic benefits—while also giving copyright holders the means to have infringing content swiftly removed without having to resort to litigation. However, it is far from the perfect solution, and there are many examples of its shortcomings.

Freedom of speech is central to the understanding of our “liberal democratic society”.²⁷⁵ It is enshrined in art.19 of the Universal Declaration of Human Rights, as well as a myriad of other international treaties and constitutional documents, including the American Constitution under the First Amendment. It is crucial that we approach intellectual property issues with this at the forefront of our mind; “[giving] those values considerable, if not overriding, weight in copyright law and policy”.²⁷⁶

For the “built-in” protections for freedom of speech in copyright law²⁷⁷ to have any real effect, there has to be an adequate means for users to be able to make use of

²⁶⁶ Google Transparency Report, <https://www.google.com/transparencyreport/removals/copyright> [Accessed 14 December 2018].

²⁶⁷ Neill and Lee, “Fixing Section 512” (2016) *American Intellectual Property Law Association Quarterly Journal*, p.2 para 2 available at <https://ssrn.com/abstract=2879696> [Accessed 14 December 2018].

²⁶⁸ Sundell “Tempting the Sword of Damocles” (2011) 12 *Minn. Journal of Law, Science, and Technology* 335, 357, para.2.

²⁶⁹ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 *Minn. Journal of Law, Science, and Technology* 387, 406, para.2.

²⁷⁰ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 *Minn. Journal of Law, Science, and Technology* 387, 406, para.3.

²⁷¹ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 *Minn. Journal of Law, Science, and Technology* 387, 406, para.3.

²⁷² Sundell, “Tempting the Sword of Damocles” (2011) 12 *Minn. Journal of Law, Science, and Technology* 335, 362, para.4.

²⁷³ Neill and Lee, “Fixing Section 512” (2016) *American Intellectual Property Law Association Quarterly Journal*, pp.10–11 available at <https://ssrn.com/abstract=2879696> [Accessed 14 December 2018].

²⁷⁴ Neill and Lee, “Fixing Section 512” (2016) *American Intellectual Property Law Association Quarterly Journal*, pp.14–15, available at <https://ssrn.com/abstract=2879696> [Accessed 14 December 2018].

²⁷⁵ Netanel, *Copyright’s Paradox* (2008), p.24, para.4.

²⁷⁶ Netanel, *Copyright’s Paradox* (2008), p.24, para.4.

²⁷⁷ *Eldred v Ashcroft* 123 S. Ct 769, 789 (2003).

them. At present, it is almost entirely dependent on the willingness of an individual online service provider to open themselves up to liability, imposing an “additional layer of censorship” into the process.²⁷⁸ In addition, despite the “flowery rhetoric”,²⁷⁹ surrounding the doctrine of fair use, the protections are often weak and inconsistent in practice,²⁸⁰ described perhaps more accurately as the “right to hire a lawyer”, rather than a reliable free speech defence.²⁸¹

The notification and takedown process is a “blunt instrument”,²⁸² and it is clear that there is a fundamental bias in the DMCA towards the interest of copyright holders.²⁸³ This, along with the lack of real consequences for submitting a fraudulent or abusive takedown results in a system that fails to give meaningful protection to the users of online platforms.²⁸⁴ Of course, while copyright

in some form is an essential mechanism to ensure the above takes place, it does not follow that the restrictive understanding that exists today is required.²⁸⁵ The expansion of copyright’s remit goes against its core purpose,²⁸⁶ and we must find ways to restrain the use of intellectual property rights online to “within their designated limits”,²⁸⁷ ensuring that “copyright’s free speech safeguards ... remain vibrant in the digital arena”.²⁸⁸

With high stakes, it is imperative that the DMCA adapts to meet the contemporary challenges that are faced with regards to copyright infringement, and freedom of speech online. The notification and takedown process is already a powerful tool, and fair use an uncertain shield to stand behind. Abuse of the provisions makes it almost impossible to fight back.

²⁷⁸ Netanel, *Copyright’s Paradox* (2008), p.127.

²⁷⁹ Netanel, *Copyright’s Paradox* (2008), p.77.

²⁸⁰ Netanel, *Copyright’s Paradox* (2008), p.77.

²⁸¹ Netanel, *Copyright’s Paradox* (2008), p.77.

²⁸² Netanel, *Copyright’s Paradox* (2008), p.77, para.3.

²⁸³ Cobia, “The Digital Millennium Copyright Act Takedown Notice Procedure” (2009) 10 Minn. Journal of Law, Science, and Technology 387, 399, para.2.

²⁸⁴ O’Donnell, “Lenz v. Universal Music Corp. and the Potential Effect of Fair Use Analysis Under the Takedown Procedures of §512 of the DMCA” (2009) 10 *Duke Law & Technology Review*, available at <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1194&context=dltr> [Accessed 3 January 2019], para.20.

²⁸⁵ Netanel, *Copyright’s Paradox* (2008), p.103.

²⁸⁶ Netanel, *Copyright’s Paradox* (2008), p.94.

²⁸⁷ Mazzone, “Copyfraud” (2006) 81 *New York University Law Review* 1026, 1031, para.1.

²⁸⁸ Netanel, *Copyright’s Paradox* (2008), p.88.

EXHIBIT D

The Importance of a Comprehensive Trademark Enforcement Program: The Changing Tides of Trademark Infringement

By Alana M. Fuierer and David P. Miranda

In recent years, online trademark infringement and counterfeiting have grown exponentially in both the United States and worldwide, posing a significant threat to authentic businesses and trademark owners, both large and small, and the global economy.

The global reach of the Internet, along with its easy access and anonymity, has allowed the Internet to become a breeding ground for trademark infringers and counterfeiters. Indeed, counterfeit goods are a global, multi-billion dollar business. For example:

- According to various reports, online counterfeiting costs the U.S. economy anywhere between \$135—\$250 billion annually.
- According to FBI, Interpol, World Customs Organization (WCO) and International Chamber of Commerce (ICC) estimates, roughly 7-8% of world trade every year is in counterfeit goods. The equivalent of about \$512 billion in global lost sales.¹
- Internet sales have seen rapid growth over the past decade. In 2014, overall U.S. retail e-commerce sales were 237 billion USD,² accounting for almost 7% of all retail sales.
- According to United Nations report, the value of counterfeit goods sold online was expected to top \$1.7 trillion by 2015.³

Given these statistics, it is clear how significant an economic impact online piracy and counterfeiting can have on U.S. businesses, and the challenges a trademark owner faces when confronted with counterfeit goods or unauthorized use of its trademarks.

In addition to the loss of revenue a business can suffer, trademark rights can become abandoned under the Lanham Act⁴ if third party infringement is tolerated and allowed to run rampant. It therefore is critical for a trademark owner to engage in vigilant policing against misuse of its marks to preserve the value of its trademarks.

Current Trends in Trademark Infringement/ Counterfeiting

As new technology and online platforms emerge, e-commerce has grown in leaps and bounds since the advent of Amazon (1994), eBay (1995) and Alibaba (1999). Technology has been a blessing and a curse for brand

owners. The market for knock-off goods has kept pace and, in some cases, has spearheaded technological advances. Indeed, counterfeiters continue to create and exploit new techniques and opportunities for selling unauthentic or pirated goods and misusing trademarks online.

It is well known that online auction sites, such as eBay, Alibaba and TaoBao, make up the primary distribution point for counterfeit products. According to one 2014 report, Chinese company Alibaba.com ranked first in market penetration, with a 23.7% global reach as of May 2014. Amazon.com, the most popular retailer in the U.S., ranked second with a 22% global reach. As of August 2015, 188 million users visited Amazon's websites per month. eBay, ranked second, had 98 million visitors during the same period.^{5,6} According to the International Anti-Counterfeiting Coalition (IACC) report in 2013, 29% of online counterfeit sales occur through eBay.⁷

By eliminating the need for brick and mortar warehouses and complex distribution channels, these sites have opened the door for individuals and sham companies to misuse valuable trademarks and make lots of money doing so. A consumer can find and buy practically anything from anywhere while sitting on his or her couch, and an online e-commerce site can exploit and feed off of a legitimate trademark owner's goodwill with impunity. Long gone are the days when Rolex is only concerned with counterfeit Rolex® watches being sold on the market streets of New York City or Big Box outlet centers. No longer can Coach only focus its efforts on knockoff Coach® purses being sold at flea markets. With the explosion of e-commerce and effective elimination of national borders via online auction sites, the barriers to widespread distribution have fallen. Born out of the rapid development of new Internet applications and platforms, increasing use of mobile devices and worldwide access to Internet bandwidth, business owners must now be prepared to face the shifting sands of e-commerce instead of street vendors and clandestine warehouses.

Faced with this reality, the following tools will help businesses and trademark owners in two important ways: (1) by minimizing online trademark infringement and counterfeits, and cutting off such misuse before it spreads and results in significant economic loss; and (2) by establishing a trademark owner who is vigilant in policing its marks against misuse, thereby protecting its mark from abandonment.

Toolkit for Policing Against Trademark Infringement, Counterfeiting and Piracy

1. Frequent and Consistent Internet Monitoring—Early Detection

While monitoring the wide variety of online sites may seem daunting, it is imperative to do so. Consistent and proactive monitoring will allow a trademark owner to stop new infringements in their tracks, before they spread. The longer an infringement has been present (and making money), the harder it is to stop without expensive litigation. Furthermore, once a new infringing item starts to spread from the original source to the hundreds, if not thousands, of third party online retail sites, it is virtually impossible to plug up all holes and you will waste valuable resources trying to do so.

Trademark infringement typically occurs *via* the hidden use of metatags, AdWords or “pay-per-click” advertising, and banner advertising. There are several ways to monitor, including manual searches on the primary search engine sites (e.g., Google®, Bing®, Dogpile®, etc.) and online auction sites (e.g., eBay®). Depending on the nature of your goods and your resources, daily, weekly or monthly monitoring may be required. Some of these sites offer no-cost, automatic search mechanisms. For example, Google offers a free service called Google Alerts, which allows you to monitor your trademarks or company’s name online. Google will send you instant results each time a specific word or phrase is used. eBay allows you to set up “Searches You Follow” and receive periodic email notifications with the search results.

Other sites have similar capabilities, free of cost. Take the time to research and use them. This information will allow you to act quickly if there is infringement or if there is an unauthorized use of your company’s trademark. You may also want to consider paying for a Trademark Watch Service.

Best Practice Tip: Early detection is always best and a good offense is the best defense. Engaging in frequent, continuous online monitoring is a best practice for every trademark owner.

2. Website Take Down Procedures

Many of the most popular online marketplaces and auction sites have comprehensive and, for the most part, user-friendly reporting mechanisms for reporting trademark and copyright infringement. These tools were put in place by the sites to avoid, or at least mitigate, liability for secondary trademark infringement and, more frequently, to comply with the Digital Millennium Copyright Act (DMCA). Secondary trademark infringement is when an online marketplace is held liable for the infringing activities of one or more of its sellers.⁸ Unfortunately for brand owners, the federal courts rarely allow a claim of secondary liability for trademark infringement to survive a motion to dismiss. Instead, the courts have made

it clear that brand owners must take some responsibility for monitoring online marketplaces and utilize the tools available.

The DMCA, passed in 1998, increases the penalties for online copyright infringement but also provides a safe harbor for Internet Service Providers (ISPs) who comply with certain “take down” procedures. As a result, these DMCA take down procedures, found on most e-commerce sites, are an important enforcement tool for intellectual property owners.

Over the past few years, online marketplace and auction sites also have initiated an increasing number of trademark infringement online reporting tools, frequently available with the DMCA tools. Examples include, Amazon, eBay, Alibaba, Etsy, Pinterest, Tublr, Houzz and Facebook. Each have their own rules, policies and oddities, and some are more complicated than others.

Perhaps one of the more exciting advancements in online trademark enforcement has been the monitoring and take-down tools provided by Alibaba®, a well-known source of counterfeit goods from China. Up until a few years ago, reporting trademark infringement or counterfeit goods through Alibaba was a frustrating waste of time and resources. Recently, Alibaba’s program for infringing content review (AliProtect) is more proactive and friendly to the trademark holder. Although AliProtect involves very specific and intricate steps an Intellectual Property Rights (IPR) holder must follow, once the IPR holder jumps through these hoops, the process can prove to be a very useful tool in stopping counterfeit products from entering the United States.

Some websites, like Amazon® and eBay®, are more conservative when it comes to taking down reported listings, while others would rather take down a listing than face the potential for secondary liability. Regardless of the success rate, these reporting mechanisms are an invaluable tool in a company’s trademark enforcement tool kit and, while not perfect, are far less expensive than filing a lawsuit.

Best Practice Tip: DMCA take down procedures must be used carefully, as the specific procedures set forth under the Copyright Act of 1976⁹ are for copyrights only. Many times, trademark owners attempt to use the DMCA procedures for alleged trademark infringements. Copyright infringement and trademark infringement are not the same. Be aware, the improper use of a DMCA takedown notice for enforcing trademarks, rather than copyrights, may constitute a violation of the DMCA (Section 512(f)) and result in monetary liability for the trademark owner.¹⁰

3. Government Programs

Trademark owners with registered trademarks on the Principal Register may record these marks with the U.S. Customs & Border Protection (CBP). Once registered, the

CBP officers can monitor imports and seize counterfeit goods that bear infringing marks at each of the ports of entry. The process for recording a registered trademark has been streamlined by the Intellectual Property Rights e-Recordation (IPRR) system, which allows trademark owners to electronically file IPR applications.¹¹

According to the CBP, in Fiscal Year 2014, there were 23,140 intellectual property rights seizures with a manufacturer's suggested retail value of \$1.2 billion.¹²

4. Other Enforcement Tools

Despite best efforts, online enforcement tools are sometimes not good enough. In those situations, a business may need to escalate to more traditional enforcement tools. This includes cease and desist letters, federal litigation (or possibly state litigation, in certain limited situations) or U.S. Patent and Trademark Office (USPTO) trademark proceedings.

For counterfeit or grey goods imported from overseas, a business can consider bringing an International Trade Commission (ITC) proceeding, which allows a trademark owner to obtain a general exclusion order preventing any and all counterfeit or infringing goods from entering the United States.

Finally, educate yourself and your employees, sales representatives, agents, customers, friends and relatives about trademark infringement, and encourage others to report infringing activity.

Best Practice Tip: One less traditional, but often times effective, tool is raising public awareness of the wrongdoing. Bad PR, or the potential for bad PR, often times will be the best form of enforcement against an entity misusing another's trademark. Do not dismiss this as a viable approach, particularly against companies who are concerned with their own brand, reputation and goodwill. However, be mindful of avoiding disparaging or disingenuous conduct that could result in liability to the trademark owner.

5. Prioritize: Identify Proper Targets and Action

While it is well settled that failure to enforce your trademark could result in abandonment or weakening of your mark, it is also impracticable to require trademark owners to prosecute each and every minor infringement.¹³ The courts do not require a business to go bankrupt policing its trademarks. As such, a strategic and tailored enforcement strategy is essential to maintaining your trademarks and it is important to prioritize your targets. Consider whether some infringements are *de minimis*, in favor of more strategic enforcement against larger, more problematic infringers. Where will you get the most bang for your enforcement dollar? Is it easier to go after the individual online retailers, or the source?

Finally, carefully consider which tool to use from the enforcement tool box. The Internet and social media not

only have changed how trademark infringers infringe, they have greatly affected how trademark owners should react. Traditionally, when trademark owners discovered a perceived infringement, they would have their attorney send out a very serious and threatening cease and desist letter. With the advent of social media, this traditional method of enforcement must be used wisely and with caution, taking into account the risk of social media backlash in each and every case, along with other factors (amount the case is worth, other ways to approach enforcement, etc.).

One more recent example of how social media can impact trademark enforcement strategies is *Lagunitas Brewing Company v. Sierra Nevada Brewing Co.* (N.D. Cal. 3:15-cv-00153). Lagunitas filed a lawsuit against Sierra Nevada on a Monday, alleging the label on Sierra Nevada's new Hop Hunter IPA was substantially similar to the design on Lagunitas's iconic IPA. Within 24 hours of Lagunitas' court filing, a social media backlash campaign spread like wildfire. By Wednesday, a mere two (2) days later, Lagunitas voluntarily dismissed the lawsuit, stating it lost its trademark case in the "Court of Public Opinion."

Best Practice Tip: There are many examples like the Lagunitas case. Once the social media train pulls out of the station, it is virtually impossible to stop or recover from the fallout. One can assume that an aggressive infringer might sometimes defiantly and publicly share a cease and desist letter from a trademark owner. It therefore is imperative that a trademark owner and its counsel be wary of the risks involved, not only with failure to enforce its trademarks, but also with overly aggressive enforcement. Think creatively. Depending on the infringer, there are various strategies and ways of protecting your marks, without necessarily resorting to threats and litigation.¹⁴

Conclusion

Absent a comprehensive, online enforcement program, trademark infringement and counterfeiting can result in significant injury to your brand, products and/or services, as well as a significant loss in revenue. The easy access to counterfeit goods out of countries like China and Russia makes it even more important to have a strategic and targeted online enforcement program in place. Early and continuous monitoring is critical to any enforcement program, as is retaining intellectual property counsel to aggressively, yet efficiently, assist with a strategic and targeted enforcement policy.

Finally, given the far reach of the Internet and fast-paced advancements in technology, it is critical for business owners to stay educated regarding new infringement methods and solutions. E-commerce and the Internet are an ever-changing and evolving platform. A trademark owner must not remain stagnant in its enforcement strategies, but must be creative, flexible and willing to change with the "piracy" tides.

Endnotes

1. *Learn About IP*, STOPFAKES.GOV, <http://www.stopfakes.gov/learn-about-ip/ip/how-serious-problem-counterfeiting-and-piracy> (last visited Mar. 20, 2016).
2. *Statistics and Facts About Global e-Commerce*, STATISTA.COM, <http://www.statista.com/topics/871/online-shopping/> (last visited Mar. 20, 2016).
3. UN INTERREGIONAL CRIME & JUSTICE RESEARCH INST. & THE INST'L CHAMBER OF COMMERCE, CONFISCATION OF THE PROCEEDS OF CRIME: A MODERN TOOL FOR DETERRING COUNTERFEITING AND PIRACY 9 (2013), http://www.unicri.it/services/library_documentation/publications/unicri_series/A_modern_tool_for_deterring_counterfeiting_and_piracy.pdf.
4. The Lanham Act, 15 U.S.C. §§ 1051-1141n (2012).
5. *Most popular retail websites in the United States as of September 2015, ranked by visitors (in millions)*, STATISTA.COM, <http://www.statista.com/statistics/271450/monthly-unique-visitors-to-us-retail-websites/> (last visited Mar. 20, 2016).
6. Sandy Smith, *The Favorite 50 2015*, NATIONAL RETAIL FEDERATION (Sept. 1, 2015), <https://nrf.com/news/the-favorite-50-2015>.
7. IACC Urges U.S. Appeals Court to Hold Ebay Contributorily Liable for Continuing Rampant Internet Sales, INTERNATIONAL ANTICOUNTERFEITING COALITION (Oct. 22, 2008), <http://www.iacc.org/announcements/iacc-urges-u-s-appeals-court-to-hold-ebay-contributorily-liable-for-continuing-rampant-internet-sale?A=SearchResult&SearchID=2178143&ObjectID=62672&ObjectType=7>.
8. In the United States, eBay and Amazon repeatedly have avoided secondary liability for trademark and copyright infringement, or counterfeiting. *See, e.g.*, *Milo & Gabby, LLC v. Amazon.com, Inc.*, 12 F.Supp. 3d 1341 (W.D. Wash. 2015); *Tiffany Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir. 2010).
9. The Copyright Act, 17 U.S.C. §§ 101-810 (2010).
10. *See* *CrossFit, Inc. v. Alvies*, No. 13-3771, 2014 WL 251760 (N.D. Cal. Jan. 22, 2014).
11. *See The Intellectual Property Rights e-Recordation (IPRR) application*, U.S. CUSTOMS AND BORDER PROTECTION, <https://iprr.cbp.gov/> (last visited Mar. 20, 2016).
12. *Intellectual Property Rights Fact Sheet*, U.S. CUSTOMS AND BORDER PROTECTION, <http://www.cbp.gov/sites/default/files/documents/IPR%20Fact%20Sheet%202014%20UPDATE%20FINAL.pdf> (last visited Mar. 20, 2016).
13. *See* *Engineered Mech. Servs. v. Applied Mech. Tech.*, 584 F.Supp. 1149 (1984) ("The owner of a mark is not required to constantly monitor every nook and cranny of the entire nation and to fire both barrels of his shotgun instantly upon spotting a possible infringer. Lawyers and lawsuits come high and a financial decision must be made in every case as to whether the gain of prosecution is worth the candle.")
14. *See, e.g.* The letter sent by Jack Daniels to an individual author, wherein Jack Daniels offered to pay for a new book cover when the book went into its 2nd reprint. Avi Dan, *The World's Nicest Cease-And-Desist Letter Ever Goes Viral, Sells Books*, FORBES (July 26, 2012, 12:38 AM), <http://www.forbes.com/sites/avidan/2012/07/26/the-worlds-nicest-cease-and-desist-letter-ever-goes-viral-sells-books/#2de713e49aca>.

Alana M. Fuierer and David P. Miranda are partners in the law firm of Heslin Rothenberg Farley & Mesiti PC. In 2006, Ms. Fuierer moved to Rochester, New York and initiated the opening of the firm's Rochester satellite office, where she has been practicing ever since. Her practice includes patent, copyright and trademark litigation, as well as patent prosecution, with technical experience in the areas of chemistry, bioremediation, environmental microbiology, hydrology, contaminant transport, materials and semiconductor design. Ms. Fuierer has been a practicing, registered patent attorney since 2002. Prior to joining Heslin Rothenberg Farley & Mesiti, PC, Ms. Fuierer was a staff attorney with the United States Court of Appeals for the 11th Circuit. She graduated *cum laude* with a Juris Doctorate from the State University of New York at Buffalo 1995, where she served on the *Buffalo Law Journal* as an Executive Editor. Ms. Fuierer also has a Bachelor's degree in Chemistry from the State University of New York at Geneseo (1992) and a Master's degree in Hydrology from the New Mexico Institute of Mining and Technology (2001).

David P. Miranda is an experienced trial attorney whose intellectual property law practice includes trademark, copyright, trade secret, false advertising, and patent infringement, as well as licensing, and internet related issues. He has litigated cases in federal district courts, state courts, the International Trade Commission, and the Trademark Trial and Appeals Board; and has successfully appeared before the Federal Circuit, Second Circuit, Ninth Circuit and New York Court of Appeals. In June 2015 Mr. Miranda began his one-year term as President of the New York State Bar Association. Mr. Miranda received his Juris Doctor degree from Albany Law School and Bachelor's degree from the State University of New York at Buffalo. He is admitted to practice in New York, U.S. District Courts for New York's Northern, Southern, Eastern and Western Districts, Massachusetts, the Federal Circuit, Second Circuit and Ninth Circuit Court of Appeals and the U.S. Supreme Court.

EXHIBIT E

Department of Commerce DMCA Multistakeholder Forum

DMCA Notice-and-Takedown Processes: List of Good, Bad, and Situational Practices

I. Good Practices

A. Good General Practices For Service Providers

1. Making DMCA takedown and counter-notice mechanisms easy to find and understand. There are many different ways to accomplish this, depending on the nature of the service in question, but some examples include ensuring that copyright takedown and counter-notice mechanisms appear readily in search engine results, are linked from web page headers and footers, and/or described in Terms of Service or Help/Contact pages;
2. Providing a clear, “plain English” explanation (consistent with DMCA requirements) of who can submit a DMCA notice and counter-notice; what information should be submitted to comply with DMCA requirements; and what additional information, if submitted, can facilitate the removal of alleged infringing content¹;
3. Implementing processes that are efficient for receiving notices that are commensurate with the volume of good faith claims of instances of infringement sought to be submitted by rights owners, for example through
 - a. allowing multiple URLs to be submitted online at one time, whether via email or a web form, that can accommodate multiple URLs, or via upload of a text file
 - b. offering, where appropriate, alternate methods of submitting notices for to large notice senders, including, for example, scalable, machine-readable processes; and/or
 - c. Additional efficiency may be achieved by establishing a standard document structure for the email or uploaded text file.
4. For notices that meet the requirements of section 512(c)(3) and relate to infringing material, or a hyperlink² to infringing material, that resides on the system or network operated by or for the service provider, providing confirmation of receipt of a notice or counter-notice that includes a method to identify the notice or counter-notice in further communications, such as a copy of the completed web form, or an email confirming that the content has been acted upon; and
5. Explaining to notice senders that DMCA notices and counter-notices are only accepted to address copyright infringement claims and are not the proper method to report other

¹ “Allegedly Infringing content” or “allegedly infringing material,” as used in this document with regard to notifications of claimed infringement, refers to material about which the notice submitter : “has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.” See 17 U.S.C. 512(c)(3)(v).

² Use of the word “links” or “linking” to infringements in the context of 512(d) notices in this document is also intended to encompass “referring” within the meaning of Section 512(d) (“referring ... users to an online location containing infringing material or infringing activity”).

legal claims (i.e. non-copyright issues such as trademark, defamation or privacy) or violations of community guidelines, terms of use, etc., and that there are legal sanctions that can apply for certain knowing and material misrepresentations in DMCA notices.

6. Making reasonable efforts, following withdrawal of the notification or receipt of a counter-notification that substantially meets the requirement of § 512(g) and where practicable, to reinstate in a timely fashion material removed pursuant to a DMCA notice.
7. If a user reposts from the same user account material that was previously removed or disabled by the service provider in response to a proper DMCA notice and the user did not submit a counter-notice in response to the DMCA notice, it is a good practice, where practicable to do so, in addition to processing the notice, for the service provider to notify the user that further reposting of the material may result in termination of the user's account.

B. Good Practices For Service Providers When Email is a Submission Mechanism

1. All Good General Practices
2. Where practicable, service providers may want to provide suggested examples of email submissions—like that in attachment A, for instance—to help notice senders send notices in a structured email format that is easier for the service provider to process.

C. Good Practices For Service Providers When a Web form is a Submission Mechanism

1. All Good General Practices
2. Web form should have clearly labeled fields and clearly mark which fields in a submission are required by the DMCA, and which fields are requested in order to allow for better processing of the notice (e.g. where multiple works appear on a single URL or where a work such as a visual image cannot readily be identified by title/author alone)
3. Providing sample text, help buttons and instructions to help explain what information is being requested;
4. Employing industry-standard features that promote efficient submission of forms such as avoiding server-side settings that would disable browser-side auto-completion features that help submitters to easily complete fields based on prior input and employing practices similar to those used as industry standards for online sales transactions wherever possible to retain properly entered data, so the notice sender does not have to re-enter it to complete a notice if certain fields on the notice have been entered incorrectly;
5. Displaying an error message upon rejection of a notice or counter-notice submission with an explanation to allow the submitter to efficiently correct the submission and resubmit the information to the service provider (except in the case of repeated submission of notices by a party that ignores an initial explanation);

D. Good General Practices for Notice Senders

1. Good faith submission of all information required by Section 512(c).
2. Submitting take down requests presented as Section 512 notices only for copyright infringement (i.e., not to address issues such as trademark, defamation, privacy, etc.).
3. Before submitting a take down notice, it is a good practice to take measures that are reasonable under the circumstances (e.g. taking into account the information visible to the notifier and the apparent volume of infringement at the location, etc.) to determine the online location at which the material or a link to the material resides and to appropriately consider whether use of the material identified in the notice in the manner complained of is not authorized by the copyright owner, its agent or the law. Using automated tools of various types to search for and send notices is a common practice to improve efficiency by notice senders who must search for numerous works across a wide variety of sites and services and send large volumes of notices. Use of such tools has evolved and will evolve over time. When using these sorts of automated tools, examples of current good practices include some combination of the following:
 - Particularly where automated takedown notices will be sent to a site based on metadata (e.g. keywords, titles, file size, etc.), conducting, in a manner reasonable under the circumstances, a human review of the site to which notices will be directed to ascertain whether the site is particularly likely or unlikely to be hosting or linking to infringing material.
 - Establishing search parameters the copyright owner or its agent believe will efficiently identify the unauthorized material while minimizing the inadvertent inclusion of authorized material; for example, in addition to searching on the title of the copyrighted work, using additional metadata (e.g. the type and size of file, etc.) where appropriate to help indicate whether material actually constitutes an unauthorized use of the copyrighted work;
 - Periodically conducting spot checks to evaluate whether the search parameters are returning the expected results, and adjusting the search parameters if needed are not as expected; and/or
 - If given sufficient information by the service provider to show that the notice sender's systems for generating notices are resulting in significant numbers of notices being sent to the service provider that do not accurately identify the online location at which the infringing material or a link to the infringing material resides or that do not accurately identify the use of the material as unauthorized, making good-faith efforts to correct the issue, with assistance from the service provider as needed, when sending further notices to the service provider.
4. Guidelines for sending DMCA notices on behalf of other parties should be developed in accordance with these best practices.

E. Good General Practices for Counter-Notice Senders

1. Before submitting a counter-notice, taking measures that are reasonable under the circumstances, consistent with DMCA section 512(g), to determine whether the material was removed or disabled as a result of a mistake or misidentification.

II. Bad Practices

A. Bad General Practices for Service Providers (Including for Both Email and Webform Submission Methods)

1. Intentionally obfuscating the procedure for submitting DMCA notices or counter-notices, such as hiding contact information for submission of take down notices or counter-notices, or placing web forms or DMCA agent's email address behind multiple click-through advertisements.
2. Requiring notice and counter-notice submitters to watch advertising, or provide anything of value as a pre-condition to submitting a notice or counter-notice.
3. Using stigmatizing or intimidating language in connection with any DMCA notice mechanism that is intended to chill submission of legitimate notices or counter-notices.
4. For service providers that host the file associated with a link identified to the service provider in a valid DMCA notice, creating multiple links to the file with the intent of frustrating the DMCA takedown process.

B. Bad General Practices for Notice Senders

1. Sending notices pursuant to DMCA Section 512(c) or (d) when the notice sender knows that the allegedly infringing material or activity: i) does not reside on a system or network controlled or operated by or for the provider within the meaning of DMCA 512(c), or ii) is not being referred or linked to by the service provider within the meaning of DMCA Section 512(d), such as when the service provider is only a 512(a) Internet access provider in the given instance or the system or network is not controlled or operated by or for the service provider.
2. Falsely asserting that the notifier is authorized to act on behalf of the owner of an exclusive right asserted.
3. Submitting invalid takedown notice requests for harassing or retaliatory purposes, such as in response to a takedown notice from the alleged poster of unauthorized material, temporarily silencing a critic, or with the goal of disrupting the service provider's takedown notification mechanism or the business of competitor or other person.
4. Submitting a DMCA take down notice to assert rights other than copyright rights (e.g., trademark, defamation, privacy, etc.).
5. Repeatedly submitting DMCA notices with regard to a URL where the rights holder knows the allegedly infringing material or hyperlink has been reposted by the service provider in response to a counter-notice meeting the requirements set forth in § 512(g)(3).

6. Engaging in a pattern or practice of failing to take reasonable efforts under the circumstances to ascertain that the allegedly infringing material appears at or is referenced at the location identified in the notice, particularly when using automated tools for scanning.
7. Falsely asserting that the notice submitter has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent or the law.
8. Intentionally submitting DMCA takedown notices in bad faith in a manner intended to obfuscate the nature of the submission or cause undue delay or hardship in processing the notice (such as, for example, sending to a fax without a cover sheet; intentionally distributing elements of a 512(c) compliant takedown notice across multiple different items of correspondence, instead of including all the information in a single notice, when the notice sender has all of this information at the time of the original notice; or sending notices by mail or by fax without a name or title of the DMCA designated agent to receive notifications etc.) with the intent of making delivery the notice to the designated agent more difficult, it being understood that it is appropriate to send notices commensurate with the volume of infringing material the notice sender seeks to have removed or blocked.
9. Sending via email bulk notices as attachments in formats that cannot easily be processed by service providers, (such as an “image-only” file whose text cannot be excerpted and copied, or converted to plain text) with the intent of making response to such notices more difficult.
10. Refusing to provide the name of the notice sender and valid contact information at an online address or phone number that the notice sender checks regularly.

C. Bad General Practices for Counter-Notice Senders

1. Falsely asserting ownership of the copyrighted work identified in the DMCA notice.
2. Submitting invalid counter notices for harassing, anti-competitive, or retaliatory purposes or for monetary or other gain.
3. Failing to take reasonable efforts to form a good faith belief that the material was removed or disabled as a result of a mistake or misidentification of the identified material.
4. Falsely asserting that the submitter of the counter notice has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the identified material.
5. Failing to provide valid contact information, including, a name, telephone number and address used regularly by the counter-notifier or their representative who will accept service of process.
6. Submitting a counter-notice when a copyright infringement lawsuit has been filed by the copyright owner against the user regarding the allegedly infringing activity and the case is pending or has been decided against the user.

III. Situational Practices (that Vary Based Upon the Situation/Context)

1. **Trusted Submitter Programs:** Where practicable for a service provider to implement, “trusted submitter” programs for submitters who have a history of submitting accurate notices can create notification efficiencies while incentivizing notifiers to follow good practices. Features of trusted submitter programs may include:
 - a. Log-in authentication mechanisms to verify the identity of reliable, accurate submitters;
 - b. Signed agreements that incorporate into each notice by reference certain information required by the DMCA that otherwise would have to be submitted each time (e.g., good faith belief, accuracy, and penalty of perjury statements);
 - c. Removal or appropriate adjustment of anti-abuse mechanisms such as CAPTCHA codes and volume and frequency limits for Trusted Submitters who have been authenticated;
 - d. Mechanisms that enable authenticated machine-to-machine submission methods, such as XML-based APIs, web form features that encourage automated submission (e.g., web forms that support text file uploads in structured formats in place of completion of web form fields); and/or
 - e. structured email formats that enable reliable, automated parsing of required information.
2. **Acknowledgement and Status Reporting:** It is a good practice for service providers to provide confirmation of receipt of notices and a method to identify notices to facilitate further communications about particular notices. In addition, where submission scale and service provider resources make it practicable, the following additional measures may lead to further efficiencies in the submission process:
 - i). Providing submitters with a record of all URLs submitted;
 - ii). Providing submitters with a record of the action taken with respect to a notice, consistent with privacy obligations.

Notices which fail to meet the requirements of section 512(c)(3) do not require and do not necessarily merit providing a confirmation or record. However, providing reasonable information to the notice sender about the deficiency of the notice (e.g. on one, but not on multiple occasions where repeated deficient notices are sent) normally promotes efficiency in both notice sending and processing by allowing sender errors to be corrected.

3. **Requesting additional information:**
 - a. Requesting additional information from the notice submitter that describes the work or a link to the legitimate version can improve efficiency in certain contexts (e.g. where title information alone may not sufficiently describe the work to allow the service provider to identify the work, or where multiple copyrighted works are available at one URL and the service provider cannot locate the works because it is not clear from the notice to which work the notice refers).
 - b. With respect to optional pieces of information, a service provider should consider informing notifiers that such information would encourage efficient submissions or

aid in identifying the works in question (e.g. where multiple works appear on a single URL or are not readily identified by the title of the work, thus frustrating efforts by the service provider to locate the allegedly infringing work).

- c. On the other hand, care should be taken not to request additional information where the notifier provides information sufficient for the service provider efficiently to identify and locate the material.
4. **Security measures**, such as CAPTCHA codes or log-in-based authentication, serve an important aim for service providers that offer online submission interfaces, namely, to protect their networks from attacks or acts of malfeasance. On the other hand, mechanisms should not be deployed in a manner intended to disrupt, or make difficult, the process of sending valid notices or counter-notices. Examples of the latter would include: (a) requiring multiple CAPTCHA codes in connection with the submission of a single notice; (b) the use of CAPTCHA codes at the conclusion of a submission in a manner that results in other data entered into the form being erased if the notice sender enters the CAPTCHA incorrectly; or (c) forcing “cool down” periods between submissions in an arbitrary manner.

It is also understood that certain security measures, including single-entry CAPTCHA requirements, can slow down the notice submission process when (a) automated systems are being used to report multiple infringements on a single system or network via an online form; or (b) a service provider only permits the submission of a single work or link via an online form before requiring the user to engage with a security measure.

Speaking to those points, service providers, depending on the resources available and the volume of valid notices they receive, may want to consider: (a) permitting the submission of multiple, instead of single, infringements in one session under a single CAPTCHA; and (b) where appropriate, alternative methods for submission of bulk alleged infringements as identified under Good and Situational Practices.

Disclaimers

These Best Practices are not intended to be, and should not be construed as, a concession or waiver with respect to any legal or policy position or as creating any legally binding rights or obligations. Stakeholders who participated in the development of these Best Practices may differ in our interpretation of relevant laws, and do not intend to resolve such differences in the Best Practices.

EXHIBIT F



[The VSCO Help Center](#) > [Account & Privacy](#) > [Privacy and Security](#)

Q Search

Private profiles on VSCO

VSCO does not offer the option to have a private profile or account at this time.

Any media that you post to your VSCO account is public for anyone to see, whether on the VSCO app or on VSCO's website, [vSCO.co](#).

Please note that any media that you import into your VSCO Studio is private and only visible to you on your device. For more information on importing media and posting to VSCO, please see our [How to use VSCO](#) article.

If you have deleted images from your VSCO profile or have deactivated your VSCO account but is still appearing in search engine results, [please read the following article on how to remove this content.](#)

[If you aren't already a VSCO Member, we invite you to join our community and try out a free 7 day trial of the VSCO Membership.](#)

Was this article helpful?

127 out of 325 found this helpful

Yes

No

Have more questions? Submit a request

Related Articles

Profile Access
Setting

How to delete a
VSCO Account

Searching on
VSCO

Visit the community.

Have a feature request? Want to interact with other creators on VSCO and the VSCO team?

Visit the Community



VSCO

TRY FOR FREE

DOWNLOAD NOW

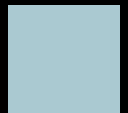
COMPANY

About VSCO

Products

Plans

Careers



Press

FEATURES

Photo Editor

Photo Filters

Mobile App

Brand Engagement

VSCO Hub

VSCO Canvas

Release Notes

COMMUNITY

What's New

Photography Community

Photographer Stories

Guidelines

Safety

Support

LEARN

Photography Basics

Photography Guides

Curated Photo Collections

Photography Business

Guides for Hiring



[Terms of Use](#)

[Privacy Policy](#)

[Studio Manager Agreement](#)

[VSCO Hub Agreement](#)

[Cookie Settings](#)

Copyright 2025 VSCO. All rights reserved.



EXHIBIT G

From: Jonathan Kleiman jonathan@jkleiman.com
Subject: Fwd: Visual Supply Company v. Adam Khimji, et al., Case No. 3:24-cv-09361 WHO
Date: January 13, 2025 at 11:50 AM
To: Adam Khimji akhimji3@uwo.ca

Jonathan Kleiman, BA, JD

1235 Bay St., Suite 700
Toronto, ON, M5R 3K4

O: 1-855-416-0416
F: 647-977-5770
M: 416-554-1639
E: Jonathan@JKleiman.com
W: www.JKleiman.com

I appreciate your reviews: <https://g.page/kleimanlaw/review?rc>

IMPORTANT NOTICE:

Funds transfer fraud is on the rise. Please note, we will never email you with a request to change or update any banking or transfer information. If you receive a request like that by email, please phone us immediately using a previously known number. In addition, if we receive any banking or transfer information from you, we will confirm this by independent means. If you have questions or concerns, please contact us at 416-554-1639.

This message and any attachment(s) are intended only for the use of the individual or entity to which they are addressed. They may contain information that is privileged, confidential and exempt from disclosure under applicable law. Distributing or copying this communication without permission of the intended recipient is strictly prohibited. If you have received this communication in error, please notify Jonathan Kleiman immediately by e-mail at Jonathan@JKleiman.com. Thank you.

----- Forwarded message -----

From: **Alinder, Zachary J.** <zalinder@sideman.com>
Date: Wed, Jan 8, 2025 at 3:01 PM
Subject: RE: Visual Supply Company v. Adam Khimji, et al., Case No. 3:24-cv-09361 WHO
To: Jonathan Kleiman <jonathan@jkleiman.com>

Thanks, Jonathan. Hope that your new year has started off smoothly!

We'll fill in 12/30 for the date sent (the date sent to Mr. Khimji directly, rather than you), and then we'll get this e-filed. I will also reach out to VSCO about re-starting the settlement discussions with you, and will revert back to you shortly.

Best,
Zac

-----Original Message-----

From: Jonathan Kleiman <jonathan@jkleiman.com>
Sent: Wednesday, January 8, 2025 11:20 AM
To: Alinder, Zachary J. <zalinder@sideman.com>
Subject: Re: Visual Supply Company v. Adam Khimji, et al., Case No. 3:24-cv-09361 WHO

Please see attached. Let me know how we can make this go away.

Thanks,

Jonathan Kleiman, BA, JD

1235 Bay St., Suite 700
Toronto, ON, M5R 3K4

O: 1-855-416-0416
F: 647-977-5770
M: 416-554-1639
E: Jonathan@JKleiman.com
W: www.JKleiman.com

I appreciate your reviews: <https://g.page/kleimanlaw/review?rc>

IMPORTANT NOTICE:

Funds transfer fraud is on the rise. Please note, we will never email you with a request to change or update any banking or transfer information. If you receive a request like that by email, please phone us immediately using a previously known number. In addition, if we receive any banking or transfer information from you, we will confirm this by independent means. If you have questions or concerns, please contact us at 416-554-1639.

This message and any attachment(s) are intended only for the use of the individual or entity to which they are addressed. They may contain information that is privileged, confidential and exempt from disclosure under applicable law. Distributing or copying this communication without permission of the intended recipient is strictly prohibited. If you have received this communication in error, please notify Jonathan Kleiman immediately by e-mail at Jonathan@JKleiman.com. Thank you.

On Fri, Jan 3, 2025 at 1:43 PM Alinder, Zachary J. <zalinder@sideman.com> wrote:

>
> Understood, thanks Jonathan. The acknowledgement of service form with the extension is not filed. He would just need to sign it and send it back to me to get the automatic extension discussed below. We have to file the form, not you or him. But if he intends to contest service, then it would be hard for me to make a case that settlement discussions now will be productive. If that is the case, then yes, he may want to get California-based counsel involved. Please let me know how Mr. Khimji would like to proceed.

>
>
>
> Best,
> Zac

>
> From: Jonathan Kleiman <jonathan@jkleiman.com>
> Sent: Friday, January 3, 2025 10:33 AM
> To: Alinder, Zachary J. <zalinder@sideman.com>
> Subject: Re: Visual Supply Company v. Adam Khimji, et al., Case No.
> 3:24-cv-09361 WHO

>
> I am only asking this as a courtesy. I am not representing him on the US file, so I won't be filing anything.

> I should let him know to get US counsel right away to not miss any deadlines then, correct?

> Jonathan Kleiman, BA, JD

> _____
> 1235 Bay St., Suite 700
> Toronto, ON, M5R 3K4

> O: 1-855-416-0416
> F: 647-977-5770
> M: 416-554-1639
> E: Jonathan@JKleiman.com
> W: www.JKleiman.com

> I appreciate your reviews: <https://g.page/kleimanlaw/review?rc>

> IMPORTANT NOTICE:

> Funds transfer fraud is on the rise. Please note, we will never email you with a request to change or update any banking or transfer information. If you receive a request like that by email, please phone us immediately using a previously known number. In addition, if we receive any banking or transfer information from you, we will confirm this by independent means. If you have questions or concerns, please contact us at 416-554-1639.

> This message and any attachment(s) are intended only for the use of the individual or entity to which they are addressed. They may contain information that is privileged, confidential and exempt from disclosure under applicable law. Distributing or copying this communication without permission of the intended recipient is strictly prohibited. If you have received this communication in error, please notify Jonathan Kleiman immediately by e-mail at Jonathan@JKleiman.com. Thank you.

> On Fri, Jan 3, 2025 at 1:29 PM Alinder, Zachary J. <zalinder@sideman.com> wrote:

> Hi Jonathan,

> Yes, there is a form included in the service package sent to both you and Mr. Khimji that allows him to get an automatic extension of time to respond. It is an obligation in our courts to reduce costs and effort on service issues, so we included the form as a courtesy. Normally that would extend the time to respond by 30 days, but because Mr. Khimji is in Canada, it would extend the time for him to respond by 60 days. My expectation is that, if we can make headway, it would be in the next month, giving him still a lot of time to obtain counsel and respond. Let me know if you see any issues with that.

> Best,
> Zac

> From: Jonathan Kleiman <jonathan@jkleiman.com>
> Sent: Thursday, January 2, 2025 6:27 PM
> To: Alinder, Zachary J. <zalinder@sideman.com>

> Subject: Re: Visual Supply Company v. Adam Khimji, et al., Case No.

> 3:24-cv-09361 WHO

>

>

>

> Please confirm.

>

>

>

> Jonathan Kleiman, BA, JD

>

>

> 1235 Bay St., Suite 700

> Toronto, ON, M5R 3K4

>

> O: 1-855-416-0416

> F: 647-977-5770

> M: 416-554-1639

> E: Jonathan@JKleiman.com

> W: www.JKleiman.com

>

> I appreciate your reviews: <https://g.page/kleimanlaw/review?rc>

>

> IMPORTANT NOTICE:

>

>

>

> Funds transfer fraud is on the rise. Please note, we will never email you with a request to change or update any banking or transfer information. If you receive a request like that by email, please phone us immediately using a previously known number. In addition, if we receive any banking or transfer information from you, we will confirm this by independent means. If you have questions or concerns, please contact us at 416-554-1639.

>

>

> This message and any attachment(s) are intended only for the use of the individual or entity to which they are addressed. They may contain information that is privileged, confidential and exempt from disclosure under applicable law. Distributing or copying this communication without permission of the intended recipient is strictly prohibited. If you have received this communication in error, please notify Jonathan Kleiman immediately by e-mail at Jonathan@JKleiman.com. Thank you.

>

>

>

>

> On Tue, Dec 31, 2024 at 6:54 PM Jonathan Kleiman <jonathan@kleiman.com> wrote:

>

> Ok thanks.

>

>

>

> I assume there is an indulgence while we see if we can settle this? Or shall I tell him to defend inside of the 30 days?

>

>

> Jonathan Kleiman, BA, JD

>

>

> 1235 Bay St., Suite 700

> Toronto, ON, M5R 3K4

>

> O: 1-855-416-0416

> F: 647-977-5770

> M: 416-554-1639

> E: Jonathan@JKleiman.com

> W: www.JKleiman.com

>

> I appreciate your reviews: <https://g.page/kleimanlaw/review?rc>

>

> IMPORTANT NOTICE:

>

> Funds transfer fraud is on the rise. Please note, we will never email you with a request to change or update any banking or transfer information. If you receive a request like that by email, please phone us immediately using a previously known number. In addition, if we receive any banking or transfer information from you, we will confirm this by independent means. If you have questions or concerns, please contact us at 416-554-1639.

>

>

> This message and any attachment(s) are intended only for the use of the individual or entity to which they are addressed. They may contain information that is privileged, confidential and exempt from disclosure under applicable law. Distributing or copying this communication without permission of the intended recipient is strictly prohibited. If you have received this communication in error, please notify Jonathan Kleiman immediately by e-mail at Jonathan@JKleiman.com. Thank you.

>

>

>

>

>

> On Tue, Dec 31, 2024 at 6:46 PM Alinder, Zachary J. <zalinder@sideman.com> wrote:

>

> Thanks for the heads up! Our delivery confirmation claims the service package was delivered, and the number 1006 was in the address, so should have been delivered to the correct apartment. He should have also received it at the protonmail email address. Any questions or issues, please don't hesitate to let me know.

issues, please don't hesitate to let me know.

> Best,

> Zac

> From: Jonathan Kleiman <jonathan@jkleiman.com>
> Sent: Tuesday, December 31, 2024 1:41 PM
> To: Alinder, Zachary J. <zalinder@sideman.com>
> Subject: Re: Visual Supply Company v. Adam Khimji, et al., Case No.
> 3:24-cv-09361 WHO

> Note that his apartment unit is #1006

> Thanks,

> Jonathan Kleiman, BA, JD

> 1235 Bay St., Suite 700
> Toronto, ON, M5R 3K4

> O: 1-855-416-0416
> F: 647-977-5770
> M: 416-554-1639
> E: Jonathan@JKleiman.com
> W: www.JKleiman.com

> I appreciate your reviews: <https://g.page/kleimanlaw/review?rc>

> IMPORTANT NOTICE:

> Funds transfer fraud is on the rise. Please note, we will never email you with a request to change or update any banking or transfer information. If you receive a request like that by email, please phone us immediately using a previously known number. In addition, if we receive any banking or transfer information from you, we will confirm this by independent means. If you have questions or concerns, please contact us at 416-554-1639.

> This message and any attachment(s) are intended only for the use of the individual or entity to which they are addressed. They may contain information that is privileged, confidential and exempt from disclosure under applicable law. Distributing or copying this communication without permission of the intended recipient is strictly prohibited. If you have received this communication in error, please notify Jonathan Kleiman immediately by e-mail at Jonathan@JKleiman.com. Thank you.

> On Mon, Dec 30, 2024 at 10:47 PM Alinder, Zachary J. <zalinder@sideman.com> wrote:

> I'll check on that and will get back to you in the new year.

> Best,

> Zac

> From: Jonathan Kleiman <jonathan@jkleiman.com>
> Sent: Monday, December 30, 2024 5:54 PM
> To: Alinder, Zachary J. <zalinder@sideman.com>
> Cc: Lee, Cindi <clee@sideman.com>; Levad, Andrew M.
> <alevad@sideman.com>
> Subject: Re: Visual Supply Company v. Adam Khimji, et al., Case No.
> 3:24-cv-09361 WHO

> Well, now that he is certain that you mean business, is there still some way to resolve it, rather than kicking it to US counsel?

> Jonathan Kleiman, BA, JD

>
> 1235 Bay St., Suite 700
> Toronto, ON, M5R 3K4
>
> O: 1-855-416-0416
> F: 647-977-5770
> M: 416-554-1639
> E: Jonathan@JKleiman.com
> W: www.JKleiman.com
>
> I appreciate your reviews: <https://g.page/kleimanlaw/review?rc>
>
> IMPORTANT NOTICE:
>
>
>
> Funds transfer fraud is on the rise. Please note, we will never email you with a request to change or update any banking or transfer information. If you receive a request like that by email, please phone us immediately using a previously known number. In addition, if we receive any banking or transfer information from you, we will confirm this by independent means. If you have questions or concerns, please contact us at 416-554-1639.
>
>
> This message and any attachment(s) are intended only for the use of the individual or entity to which they are addressed. They may contain information that is privileged, confidential and exempt from disclosure under applicable law. Distributing or copying this communication without permission of the intended recipient is strictly prohibited. If you have received this communication in error, please notify Jonathan Kleiman immediately by e-mail at Jonathan@JKleiman.com. Thank you.
>
>
>
>
> On Mon, Dec 30, 2024 at 7:56 PM Alinder, Zachary J. <zalinder@sideman.com> wrote:
>
> Thanks for the quick response, Jonathan! While I understand that you cannot represent him in California, just to be clear, that doesn't change that you have been representing him as legal counsel or that serving his legal counsel likely constitutes adequate service/notice for Mr. Khimji directly. However, in an abundance of caution, we will also send to him directly. Putting that aside, I do hope that you are able to continue advising him going forward in some capacity, as I did think that our prior direct discussions were promising, even if not ultimately productive.
>
>
>
> Hope you have a Happy New Year in the meantime!
>
>
>
> Best,
>
> Zac
>
>
>
> From: Jonathan Kleiman <jonathan@jkleiman.com>
> Sent: Monday, December 30, 2024 2:38 PM
> To: Lee, Cindi <clees@sideman.com>
> Cc: Alinder, Zachary J. <zalinder@sideman.com>; Levad, Andrew M. <alevad@sideman.com>
> Subject: Re: Visual Supply Company v. Adam Khimji, et al., Case No. 3:24-cv-09361 WHO
>
>
>
> You will need to serve them directly as I cannot assist with this.
>
>
> Jonathan Kleiman, BA, JD
> _____
>
> 1235 Bay St., Suite 700
> Toronto, ON, M5R 3K4
>
> O: 1-855-416-0416
> F: 647-977-5770
> M: 416-554-1639
> E: Jonathan@JKleiman.com
> W: www.JKleiman.com
>
> I appreciate your reviews: <https://g.page/kleimanlaw/review?rc>
>
> IMPORTANT NOTICE:
>
>
> Funds transfer fraud is on the rise. Please note, we will never email you with a request to change or update any banking or transfer information. If you receive a request like that by email, please phone us immediately using a previously known number. In addition, if we receive any banking or transfer information from you, we will confirm this by independent means. If you have questions or concerns, please contact us at 416-554-1639.
>
>
> This message and any attachment(s) are intended only for the use of the individual or entity to which they are addressed. They may

> This message and any attachment(s) are intended only for the use of the individual or entity to which they are addressed. They may contain information that is privileged, confidential and exempt from disclosure under applicable law. Distributing or copying this communication without permission of the intended recipient is strictly prohibited. If you have received this communication in error, please notify Jonathan Kleiman immediately by e-mail at Jonathan@JKleiman.com. Thank you.

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

>

> On Mon, Dec 30, 2024 at 5:29 PM Lee, Cindi <clees@sideman.com> wrote:

> Counsel:

> Please see the attached documents. Thank you.

> Cindi Lee

> I

> Legal Assistant

> San Francisco, CA

> Main: 415.392.1960

> clees@sideman.com

> www.sideman.com

> CONFIDENTIALITY

> This e-mail may contain confidential and privileged material for the sole use of the intended recipient(s). Any review, use, distribution or disclosure by others is strictly prohibited. If you are not the intended recipient (or authorized to receive for the recipient), please contact the sender by reply e-mail [or at (415) 392-1960] and delete all copies of this message. It is the recipient's responsibility to scan this e-mail and any attachments for viruses.